TEORIA INTUITIVA DE LOS CONJUNTOS

EDICION CORREGIDA

8a. IMPRESION

PAUL R. HALMOS

C. E. C. S. A.

Landau: Fundamentos de analisis moderno ESTADI...

Robin: Principios analisis matematico. Algebra II

TEORIA INTUITIVA DE LOS CONJUNTOS

T. I. De los C.

CALCULO III Lunes a Viernes de 5-6 (6-7), S. 124

Algebra II Lunes a Viernes de 4-5, S 115

Geom. Anal. Lunes a Viernes de 3-4, S 207

Fisica Clas. Lunes y Miercoles, S 102 de 7 a 8

ALGEBRA LIN ... y Juev., S 103 de 6 a 8

4 al 2 - 106 Lab Viernes S E de 6 a 9

L Ma Mi de 5-7 CAL

Ju de 5-6

Vi de 5-7

L Mier de 7 a 8 Fis.

Ma Jue de 6-8

Viernes de 6 a 9

Nueva York 33 A

Núm. altos 203 ó 313

Elias Selem Avila

Cal. Napoles.

TEORIA INTUITIVA DE LOS CONJUNTOS

Por

PAUL R. HALMOS

Profesor de Matemáticas en la Universidad de Michigan

COMPAÑIA EDITORIAL CONTINENTAL, S. A.

MEXICO – ESPAÑA – ARGENTINA – CHILE

SUCURSALES, DEPOSITOS Y REPRESENTACIONES EN:

Bolivia – Brasil – Colombia – Costa Rica – Dominicana – Ecuador – El Salvador
Estados Unidos – Guatemala – Honduras – Nicaragua – Panamá – Paraguay – Perú
Portugal – Puerto Rico – Uruguay – Venezuela

Título original en inglés:
NAIVE SET THEORY

Traducido por:
Ing. ANTONIO MARTIN–LUNAS
Director del Instituto Particular de Estudios Matemáticos, México

Revisado por:
ANDRES SESTIER BOUCLIER
Maestro en Ciencias del Centro de Investigaciones y Estudios Avanzados del Instituto Politécnico Nacional, México

Edición autorizada por:
D. VAN NOSTRAND COMPANY, INC.
Princeton, New Jersey

Library of Congress Catalog Card Number 60-11059

Primera edición en español: mayo de 1965

Impresiones de la primera edición en español:
diciembre de 1965; octubre de 1966; septiembre de 1967; enero de 1969

Sexta impresión en español, revisada y corregida: julio de 1971

Séptima impresión en español: julio de 1972

Octava impresión en español:
abril de 1973

COMPAÑIA EDITORIAL CONTINENTAL, S. A.
CALZ. DE TLALPAN NÚM. 4620, MÉXICO 22, D. F.

MIEMBRO DE LA CAMARA NACIONAL DE LA INDUSTRIA EDITORIAL
Registro Núm. 43

AV. REP. ARGENTINA NÚM. 168, BARCELONA 6, ESPAÑA
SOLÍS NÚM. 1262, BUENOS AIRES, ARGENTINA
AMUNÁTEGUI NÚM. 458, SANTIAGO DE CHILE, CHILE

IMPRESO EN MEXICO PRINTED IN MEXICO

PREFACIO

Los matemáticos están de acuerdo en que cada uno de ellos debe saber algo de teoría de conjuntos; el desacuerdo comienza al tratar de decidir qué tanto es algo. Este libro contiene mi respuesta a esa pregunta. El propósito del libro es el de comunicar al principiante en matemáticas avanzadas, los hechos básicos en la vida acerca de la teoría de los conjuntos y hacerlo con el mínimo de raciocinio filosófico y formalismo lógico. El punto de vista de principio a fin es el de un futuro matemático ansioso de estudiar grupos, o integrales, o variedades. Desde este punto de vista, los conceptos y métodos de este libro son tan sólo algunas de las herramientas usuales de las matemáticas; el especialista experto no encontrará nada nuevo aquí.

Los créditos académicos y referencias bibliográficas están fuera de lugar en un libro puramente expositivo como el presente. Sin embargo, el estudiante que se interese en la teoría de los conjuntos en sí debe saber que existe mucho más al respecto que lo que se encuentra en este libro. Una de las más bellas fuentes de conocimientos en la teoría de los conjuntos sigue siendo la *Teoría de los Conjuntos* de Hausdorff. Una adición a la literatura reciente y sumamente amena, con una extensa bibliografía actualizada es la *Teoría Axiomática de los Conjuntos*, de Suppes.*

En la teoría de los conjuntos "intuitivo" ** y "axiomático" son palabras contrastantes. El estudio presente podría describirse mejor como una teoría axiomática de los conjuntos desde el punto de vista intuitivo. Es axiomática por el hecho de que algunos axiomas de la teoría de los conjuntos son propuestos y usados como base para todas las demostraciones subsecuentes. Es intuitiva porque el lenguaje y las notaciones son los usados en las matemáticas ordinarias informales (pero formalizables). Un aspecto más importante en el cual predomina el punto de vista intuitivo es que la teoría de los conjuntos es considerada como una colección de hechos de la cual los axiomas son un sumario breve y conveniente; en el enfoque axiomático conven-

* Título original en inglés: *Axiomatic Set Theory*.

** En el original aparece *naïve* que en francés significa *ingenua*. (N. del R.)

cional las relaciones lógicas entre varios axiomas son los puntos centrales de estudio. Análogamente, un estudio de geometría podría ser considerado como puramente intuitivo si procediera del desenvolvimiento de la sola intuición; el otro extremo, el puramente axiomático, es aquel en el cual axiomas de las diversas geometrías no euclidianas son estudiados con la misma atención que los de Euclides. El análogo del punto de vista de este libro es el estudio de un solo conjunto sensato de axiomas con la intención de describir únicamente geometría euclidiana.

En lugar de *Teoría Intuitiva de los Conjuntos*, un título más honesto para el libro habría sido *Un esbozo de los Elementos de la Teoría Intuitiva de los Conjuntos*. La palabra "elementos" dejaría ver al lector que no todo se incluye aquí, y la palabra "esbozo" lo prevendría en el sentido de que aún lo que se incluye necesita ser completado. El estilo es usualmente informal con el objeto de beneficiar la conversación. Muy pocos teoremas son presentados; la mayoría de los hechos sólo son propuestos y seguidos de un bosquejo de demostración, en forma muy parecida a como estarían en una lectura descriptiva general. Hay sólo unos cuantos ejercicios señalados expresamente como tales pero, de hecho, la mayor parte del libro no es otra cosa que una larga cadena de ejercicios con sugerencias. El lector debe preguntarse continuamente a sí mismo si está o no en condiciones de pasar de una sugerencia a la siguiente y, en relación a ello, no debe desanimarse si encuentra que su rapidez de asimilación es más baja que la acostumbrada.

Esto no quiere decir que el contenido de este libro es especialmente difícil o profundo. Lo que pasa es que los conceptos son muy generales y muy abstractos, por lo cual, es posible que le tome algún tiempo acostumbrarse a ellos. Sin embargo, es un hecho en matemáticas que un teorema es menos profundo cuanto más generalmente se aplica. La tarea del estudiante al aprender teoría de conjuntos es la de empaparse en generalidades poco familiares, pero esencialmente superficiales, hasta que se acostumbre tanto a ellas que pueda usarlas casi sin esfuerzo consciente. En otras palabras, la teoría general de los conjuntos en realidad es un material bastante trivial, pero, si usted quiere ser un matemático, necesita algo de esta teoría, y aquí está; léala, absórbala y olvídela.

P.R.H.

CONTENIDO

SECCION 1

EL AXIOMA DE EXTENSION

Una manada de lobos, un racimo de uvas o una bandada de pichones son ejemplos de conjuntos de objetos. El concepto matemático de un conjunto puede ser usado como el fundamento de todas las matemáticas conocidas. El propósito de este pequeño libro es el de desarrollar las propiedades básicas de los conjuntos. Incidentalmente, para evitar una monotonía terminológica, algunas veces diremos *colección* en vez de *conjunto*. La palabra "clase" también es usada en este contexto; pero hay cierto riesgo al hacerlo. La razón es que en algunos tratamientos de la teoría de los conjuntos, la palabra "clase" tiene un significado técnico especial. Un poco más adelante tendremos ocasión de referirnos a esto nuevamente.

La definición de conjunto es algo que no será incluido en el presente desarrollo. Esto es algo análogo a lo que ocurre en el tratamiento familiar que se da de la geometría elemental. Dicho tratamiento no ofrece una definición de puntos y rectas, sino que, en lugar de ello, describe qué es lo que uno puede hacer con esos objetos. Para el punto de vista semiaxiomático que aquí se adopta, se supone que el lector posee el entendimiento ordinario, humano, intuitivo (y frecuentemente erróneo) de lo que son los conjuntos; el propósito de la exposición es el de delinear algunas de las muchas cosas que uno puede hacer correctamente con ellos.

Los conjuntos, como se les concibe usualmente, tienen *elementos* o *miembros*. Un elemento de un conjunto puede ser un lobo, una uva o un pichón. Es importante saber que un conjunto mismo puede ser también un elemento de algún otro conjunto. En las matemáticas se encuentra un sinnúmero de ejemplos

de conjuntos de conjuntos. Una recta, por ejemplo, es un conjunto de puntos; el conjunto de todas las rectas del plano es un ejemplo natural de conjunto de conjuntos (de puntos). Más que el hecho de que los conjuntos puedan presentarse como elementos, quizá resulte sorprendente el que, para fines matemáticos, ningún otro tipo de elementos necesita ser considerado. En este libro, particularmente, estudiaremos conjuntos y conjuntos de conjuntos y torres semejantes de altura y complejidad imponentes en ocasiones —y nada más. En calidad de ejemplos, podríamos ocasionalmente hablar de conjuntos de coles, de reyes y de cosas por el estilo, pero tal costumbre debe ser interpretada siempre sólo como una parábola ilustrativa y no como parte de la teoría que esté siendo desarrollada.

El concepto principal de la teoría de los conjuntos, aquel que en estudios completamente axiomáticos es el concepto primitivo principal (indefinido), es el de *pertenencia*. Si x pertenece a A (x es un elemento de A, x está *contenido* en A), escribiremos

$$x \in A.$$

Esta versión de la letra griega épsilon es tan usada para denotar pertenencia, que su empleo para denotar cualquier otra cosa está casi prohibido. La mayoría de los autores reservan a $\in$ para usarlo siempre en la teoría de los conjuntos y ε cuando necesitan la quinta letra del alfabeto griego.

Quizá resulte útil una pequeña disgresión acerca del empleo del alfabeto en la teoría de los conjuntos. No existe ninguna razón de peso para emplear letras minúsculas y mayúsculas como se hizo en el párrafo anterior; podríamos haber escrito, y a menudo lo haremos, cosas como $x \in y$ y $A \in B$. Sin embargo, siempre que sea posible, indicaremos informalmente la posición relativa de un conjunto en una jerarquía particular bajo consideración, en términos de la convención de que las primeras letras del alfabeto denotarán elementos y las últimas conjuntos que los contienen; análogamente, letras de un tipo relativamente sencillo denotarán elementos, mientras que las del tipo más llamativo o estilizado denotarán conjuntos que los contienen. Ejemplos: $x \in A$, $A \in X$, $X \in \mathcal{C}$.

Una relación posible entre conjuntos, más elemental que la de pertenencia, es la de *igualdad*. La igualdad entre dos conjuntos A y B se denota universalmente por el conocido símbolo

$$A = B;$$

y el hecho de que A y B no son iguales se expresa escribiendo

$$A \neq B.$$

La propiedad más importante de la pertenencia es su relación con la igualdad, misma que puede formularse de la manera siguiente:

Axioma de la extensión. *Dos conjuntos son iguales si y sólo si tienen los mismos elementos.*

Con mayor pretensión y menos claridad: un conjunto está determinado por su extensión.

Es valioso comprender que el axioma de la extensión no es sólo una propiedad lógicamente necesaria de la igualdad, sino que es una proposición no trivial acerca de la pertenencia. Una manera de llegar a entender el punto es la de considerar una situación parcialmente semejante en la cual el análogo del axioma de la extensión no se cumpla. Supóngase, por ejemplo, que consideramos seres humanos en lugar de conjuntos y que, si x y A son seres humanos, escribimos $x \in A$ siempre que x es un ancestro de A. (Los ancestros de un ser humano son sùs padres, los padres de sus padres, los padres de éstos, etc., etc.) El análogo del axioma de la extensión diría en este caso que si dos seres humanos son iguales, tienen los mismos ancestros (ésta sería la parte "sólo si", y es verdadera) y, también, que si dos seres humanos tienen los mismos ancestros, entonces son iguales (ésta es la parte "si", y es falsa).

Si A y B son dos conjuntos y todo elemento de A es un elemento de B, decimos que A es un *subconjunto* de B o que B *incluye* a A, y escribimos

$$A \subset B$$

o

$$B \supset A.$$

El enunciado de la definición implica que todo conjunto debe considerarse incluido en sí mismo ($A \subset A$); este hecho se describe diciendo que la inclusión es *reflexiva*. (Nótese que, en el mismo sentido de la palabra, la igualdad también es reflexiva). Si A y B son dos conjuntos tales que $A \subset B$ y $A \neq B$, la palabra *propio* (*a*) es usada (subconjunto propio, inclusión propia). Si A, B y C son tres conjuntos tales que $A \subset B$ y $B \subset C$, entonces $A \subset C$; este hecho se describe diciendo que la inclusión entre conjuntos es *transitiva*. (También la igualdad posee esta propiedad).

Si A y B son dos conjuntos tales que $A \subset B$ y $B \subset A$, entonces A y B tienen los mismos elementos y, por lo tanto, en virtud del axioma de la extensión, $A = B$. Este hecho se describe diciendo que la inclusión de conjuntos es *antisimétrica*. (A este respecto, la inclusión entre conjuntos se comporta en forma distinta a la igualdad. La igualdad es *simétrica* en el sentido de que si $A = B$ entonces, necesariamente, $B = A$.) De hecho, el axioma de la extensión puede ser formulado en estos términos: si A y B son dos conjuntos, una condición necesaria y suficiente para que $A = B$ es que $A \subset B$ y $B \subset A$ simultáneamente. De manera correspondiente, casi todas las demostraciones de igualdades entre dos conjuntos A y B están divididas en dos partes; hacer ver primero que $A \subset B$, y mostrar después que $B \subset A$.

Obsérvese que la pertenencia (ϵ) y la inclusión ($\subset$) son, conceptualmente, cosas muy diferentes. Una diferencia importante se ha manifestado ya por sí misma anteriormente: la inclusión es siempre reflexiva, mientras que no está del todo claro que la pertenencia llegue a serlo. Esto es: $A \subset A$ es siempre cierto; pero, ¿será siempre cierto que $A \epsilon A$? Indudablemente que no lo es para ningún conjunto razonable que persona alguna haya considerado alguna vez. Obsérvese, en este contexto, que la inclusión es transitiva, mientras que la pertenencia no lo es. Ejemplos de la vida diaria, concernientes, digamos, a superorganizaciones cuyos miembros son organizaciones, se presentarán prontamente al lector interesado.

SECCION 2

EL AXIOMA DE LA ESPECIFICACIÓN

Todos los principios básicos de la teoría de los conjuntos, con la sola excepción del axioma de la extensión, están diseñados para la formación de nuevos conjuntos a partir de los originales. El primero y más importante de estos principios básicos en la manufactura de conjuntos dice, hablando toscamente, que cualquier cosa sensata que pueda uno proponer para los elementos de un conjunto, define un subconjunto, a saber, el subconjunto de aquellos elementos para los cuales la proposición es verdadera.

Antes de formular este principio en términos precisos, enfocaremos un ejemplo heurístico. Sea A el conjunto de todos los hombres. La frase "x es casado" es verdadera para algunos de los elementos x de A y falsa para otros. El principio que estamos ilustrando es aquel que justifica el paso del conjunto A al subconjunto especificado por la cláusula dada (o sea, al conjunto de todos los hombres casados). La caracterización del subconjunto se indica usualmente con la notación

$$\{x \in A: x \textit{ es casado}\}$$

Análogamente

$$\{x \in A: x \textit{ no es casado}\}$$

es el conjunto de todos los solteros;

$$\{x \in A: \textit{el padre de } x \textit{ es Adán}\}$$

es el conjunto que contiene a Caín v Abel y nada más; y

$$\{x \in A: x \textit{ es el padre de Abel}\}$$

es el conjunto que contiene a Adán y nada más. Cuidado: una caja que contiene un sombrero y nada más, no es lo mismo que un sombrero y, análogamente, el último conjunto de la anterior lista de ejemplos no debe ser confundido con Adán. La analogía entre conjuntos y cajas tiene muchos puntos débiles, pero, a veces, proporciona un cuadro útil de la situación.

Todo lo que falta para la formulación general precisa que fundamenta los ejemplos anteriores es una definición de *frase,* He aquí una rápida e informal. Hay dos tipos básicos de *frases,* a saber, *proposiciones* de pertenencia,

$$x \epsilon A,$$

y *proposiciones* de igualdad,

$$A = B;$$

todas las demás frases se obtienen a partir de las frases atómicas* por medio de aplicaciones repetidas de los operadores lógicos usuales, sujetas únicamente a las mínimas exigencias de la gramática y la claridad. Para hacer más explícita la definición (y más larga) es necesario agregarle una lista de los "operadores lógicos usuales" y las reglas de la sintaxis. Una lista adecuada (y, de hecho, redundante) de los primeros, contiene siete de ellos:

y,
o (en el sentido de "*cualquiera—o—o ambos*"),
no
si –entonces—(o *implica*),
si y sólo si,
para algún, (o *existe*)
para todo

En cuanto a las reglas para la construcción de las frases, pueden ser descritas de la manera siguiente: (i) Escriba "no" antes de una frase y encierre el resultado entre paréntesis. (El objeto de los paréntesis, aquí y en lo sucesivo, es el de evitar ambigüedades. Incidentalmente, obsérvese que éstos hacen innecesarios a todos los demás signos de puntuación. Raramente se hace necesario el juego completo de paréntesis que requiere la definición de frase. Omitiremos tantos paréntesis como sea posible sin dar lugar a confusiones. En la práctica nor-

*El autor usa la palabra "atómicas" en el sentido de "elementales", "primarias" (N. del T.)

mal de las matemáticas, que se seguirá en este libro, se usan distintos tipos y tamaños de paréntesis, pero sólo por conveniencia visual.) (ii) Escriba "y" u "o", o "si y sólo si" entre dos frases y encierre el resultado entre paréntesis. (iii) Reemplace los guiones en "si—entonces—" por frases y encierre el resultado entre paréntesis. (iv) Reemplace el guión en "para algún—" o en "para todo—" por una letra, siga el resultado por una frase y encierre todo entre paréntesis. (Nada malo sucede si la letra empleada no se presenta en la frase. De acuerdo con la convención usual y natural "para algún y $(x \in A)$" significa simplemente "$x \in A$". Es igualmente inofensivo que la letra usada haya sido empleada anteriormente con "para algún—" o "para todo—". Recuérdese que "para algún x $(x \in A)$" significa lo mismo que "para algún y $(y \in A)$"; de aquí se sigue que un cambio de notación sensato evitará siempre las colisiones alfabéticas).

Estamos ahora en posibilidades de enunciar el principio más importante de la teoría de los conjuntos, al cual se le llama a veces por su nombre alemán *Aussonderungsaxiom*.

Axioma de la especificación. *A todo conjunto A y a toda condición S(x) corresponde un conjunto B cuyos elementos son precisamente aquellos elementos x de A para los cuales se cumple S(x).*

Una "condición" es aquí simplemente una frase. La intención del simbolismo es la de indicar que la letra x es *libre* en la frase $S(x)$, lo cual significa que x tiene lugar en $S(x)$ cuando menos una vez sin necesidad de ser introducida por una de las frases "para algún x" "para todo x". Una consecuencia inmediata del axioma de la extensión es que el axioma de la especificación determina unívocamente al conjunto B. Para indicar la forma en que B es obtenido a partir de A y de $S(x)$, se acostumbra escribir

$$B = \{x \in A : S(x)\}.$$

Para obtener una aplicación divertida e instructiva del axioma de la especificación, considérese, en el papel de $S(x)$, a la frase.

$$\text{no } (x \in x).$$

Será conveniente aquí y en lo sucesivo, escribir "$x \epsilon' A$" (alternativamente con "$x \notin A$") en lugar de "no $(x \epsilon A)$"; con esta notación, el papel de $S(x)$ es jugado ahora por

$$x \epsilon' x.$$

De ahí se sigue que, cualquiera que sea el conjunto A, si $B = \{x \epsilon A: x \epsilon' x\}$, entonces, para toda y,

(*) $y \epsilon B$ *si* y *sólo si* $(y \epsilon A$ y $y \epsilon' y)$.

¿Será posible que $B \epsilon A$? Procederemos a demostrar que la respuesta es no. En efecto, si $B \epsilon A$, entonces, o $B \epsilon B$ también (lo cual es improbable pero no obviamente imposible), o bien $B \epsilon' B$. Si $B \epsilon B$, entonces, por (*), la suposición $B \epsilon A$ implica que $B \epsilon' B$—lo cual es una contradicción. Si $B \epsilon' B$, entonces otra vez por (*), la suposición $B \epsilon A$ implica que $B \epsilon B$—lo cual es, otra vez, una contradicción. Esto completa la demostración de que es imposible que $B \epsilon A$, por lo cual debemos tener que $B \epsilon' A$. La parte más interesante de esta conclusión es el hecho de que existe algo (es decir, B) que no pertenece A. El conjunto A en este razonamiento fue completamente arbitrario. Hemos demostrado, en otras palabras, que

no hay algo que contenga a todo,

o, más espectacularmente, que

no hay universo.

"Universo" se usa aquí en el sentido de "universo de discurso", lo cual significa, en cualquier discusión particular, un conjunto que contiene a todos los objetos que intervienen en ese estudio.

En tratamientos más antiguos (preaxiomáticos) a la teoría de los conjuntos, se daba por supuesta la existencia de un universo, y el razonamiento del párrafo anterior se conocía como la *paradoja de Russell*. La moraleja es que es imposible, especialmente en matemáticas, obtener algo a partir de nada. Para especificar un conjunto, no basta pronunciar algunas palabras mágicas (las cuales pueden formar una frase tal como "$x \epsilon' x$"); es necesario también disponer de un conjunto a cuyos elementos puedan aplicarse esas palabras mágicas.

SECCION 3

PAREJAS NO ORDENADAS

Por todo lo que se ha dicho hasta ahora, podríamos haber estado especulando en un vacío. Para dar sustancia a la discusión, supongamos ahora oficialmente que

existe un conjunto.

Ya que más adelante formularemos una suposición de existencia más profunda y más útil, la presente juega sólo un papel temporal. Una consecuencia de esta aparentemente innocua suposición es la de que existe un conjunto sin elementos. En efecto, si A es un conjunto, aplíquele el axioma de la especificación con la frase "$x \neq x$" (o, para el caso, con cualquier otra frase universalmente falsa). El resultado es el conjunto $\{x \in A: x \neq x\}$, y este conjunto, evidentemente, no tiene elementos. El axioma de la extensión implica que sólo puede haber un conjunto sin elementos. El símbolo usual para dicho conjunto es

$$\varnothing;$$

y se le llama *conjunto vacío.*

El conjunto vacío es un subconjunto de todo conjunto, o, en otras palabras, $\varnothing \subset A$ para todo A. Para establecer esto, podemos razonar de la siguiente manera: se trata de demostrar que todo elemento de $\varnothing$ pertenece a A; pero como no hay elementos en $\varnothing$, la condición queda satisfecha automáticamente. El razonamiento es correcto, pero tal vez poco satisfactorio. Como éste es un ejemplo típico, de una condición que se cumple en el sentido de "vacuidad", parece oportuno dar una infor-

mación al lector inexperto. Para demostrar que es cierto algo acerca del conjunto vacío, demuestre que no puede ser falso. Por ejemplo, ¿cómo puede ser falso que $\varnothing \subset A$? Sería falso sólo si $\varnothing$ tuviera un elemento que no perteneciera a A. Como $\varnothing$ no tiene elemento alguno, esto es absurdo. Conclusión: $\varnothing \subset A$ no es falso, y, por consiguiente, $\varnothing \subset A$ para todo A.

La teoría de los conjuntos desarrollada hasta ahora, es aún muy pobre, pues todo lo que sabemos es que hay un solo conjunto y éste es vacío. ¿Habrá suficientes conjuntos para garantizar que todo conjunto es un elemento de algún conjunto? ¿Será cierto que para dos conjuntos cualesquiera existe un tercero al cual pertenecen ambos? ¿Y qué hay acerca de tres conjuntos, o de cuatro, o de cualquier número? Necesitamos un nuevo principio de construcción de conjuntos para contestar esas preguntas. El siguiente principio es un buen comienzo.

Axioma del apareamiento. *Para dos conjuntos cualesquiera, existe un conjunto al cual pertenecen ambos.*

Nótese que esto es precisamente la respuesta afirmativa a la segunda de las preguntas anteriores.

Para tranquilizar las inquietudes, indicamos desde luego que palabras tales como "dos", "tres" y "cuatro", usadas anteriormente, no se refieren a los conceptos matemáticos que llevan estos nombres, mismos que serán definidos más adelante, sino que, por ahora, tales palabras son meramente las abreviaturas lingüísticas ordinarias para "algo y después algo más" repetido un número apropiado de veces. Así, por ejemplo, el axioma del apareamiento, expresado en forma no abreviada, dice que si a es un conjunto y b es otro conjunto, entonces existe un conjunto A tal que $a \in A$ y $b \in A$.

Una consecuencia (de hecho, una formulación equivalente) del axioma del apareamiento es que, para dos conjuntos cualesquiera, existe un conjunto que los contiene a ambos y nada más. En efecto, si a y b son dos conjuntos y si A es un conjunto tal que $a \in A$ y $b \in A$, podemos aplicarle a A el axioma de la especificación con la cláusula "$x = a$ o $x = b$". El resultado es el conjunto

$$\{x \in A : x = a \text{ o } x = b\},$$

y este conjunto, obviamente, contiene sólo a a y b. El axioma de la extensión implica que sólo puede haber un conjunto con esta propiedad. El símbolo usual para el mismo es

$$\{a, b\};$$

y se le llama la *pareja* (o, a modo de comparación enfática con un concepto subsecuente, la *pareja no-ordenada*) formada por a y b.

Si, temporalmente, nos referimos a la cláusula "$x = a$ o $x = b$" por medio de $S(x)$, podemos expresar el axioma del apareamiento diciendo que existe un conjunto B tal que

(*) $$x \in B \text{ si y sólo si } S(x).$$

El axioma de la especificación aplicado a un conjunto A, garantiza la existencia de un conjunto B tal que

(**) $$x \in B \text{ si y sólo si } [x \in A \text{ y } S(x)]).$$

La relación entre (*) y (**) es ejemplo de algo que ocurre con frecuencia. Todos los principios restantes en la construcción de conjuntos son casos pseudoespeciales del axioma de la especificación, en el sentido en el que (*) es un caso pseudoespecial de (**). Todos ellos garantizan la existencia de un conjunto especificado por una cierta condición; si se supiera de antemano que existe un conjunto que contiene a todos los elementos especificados, entonces la existencia de un conjunto que los contiene sólo a ellos se seguiría como un caso especial del axioma de la especificación.

Si a es un conjunto, podemos formar la pareja no-ordenada $\{a, a\}$. Esta pareja no-ordenada es denotada por

$$\{a\}$$

y se le llama conjunto singular[1] de a, estando caracterizado en forma única por el hecho de que su único elemento es a. De aquí que, por ejemplo, $\varnothing$ y $\{\varnothing\}$ son dos conjuntos muy diferentes, ya que el primero no tiene elemento alguno mientras que el último tiene a $\varnothing$ como único elemento. Decir que $a \in A$ equivale a decir que $\{a\} \subset A$.

El axioma del apareamiento asegura que todo conjunto es un elemento de algún conjunto y que dos conjuntos cua-

[1] La voz inglesa "singleton", con que el autor denota este conjunto, por no existir en castellano una traducción apropiada, se ha considerado pertinente traducirla por "conjunto singular". (N. del T.)

lesquiera son simultáneamente elementos de algún mismo conjunto. (La preguntas correspondientes para tres, cuatro y más conjuntos, serán contestadas más adelante.) Otro comentario pertinente es que, a partir de las suposiciones que hemos hecho hasta ahora, podemos inferir la existencia de muchísimos conjuntos. Considérense como ejemplos los conjuntos $\varnothing$, $\{\varnothing\}$, $\{\{\varnothing\}\}$, $\{\{\{\varnothing\}\}\}$, etc.; considérense las parejas tales como $\{\varnothing, \{\varnothing\}\}$, formadas por dos cualesquiera de ellos; considérense las parejas formadas por dos cualesquiera de las parejas anteriores, o bien, las parejas mixtas formadas por cualquier conjunto singular y cualquier pareja; y proceda indefinidamente de esta manera.

> EJERCICIO. ¿Son distintos entre sí todos los conjuntos obtenidos en esa forma?

Antes de continuar nuestro estudio de la teoría de los conjuntos, haremos una breve pausa para tratar un asunto referente a notaciones. Parece natural denotar al conjunto B descrito en (*) por $\{x: S(x)\}$, de manera que, en el caso especial que ahí fue considerado,

$$\{x : x = a \text{ o } x = b\} = \{a, b\}.$$

Usaremos este simbolismo siempre que sea conveniente y permisible hacerlo. Esto es, que si $S(x)$ es una condición sobre x tal que los "equis" especificados por $S(x)$ constituyan un conjunto, entonces denotaremos dicho conjunto por

$$\{x: S(x)\}.$$

En el caso en que A es un conjunto y $S(x)$ es $(x \in A)$, está permitido formar $\{x : S(x)\}$; de hecho

$$\{x: x \in A\} = A.$$

Si A es un conjunto y $S(x)$ una frase arbitraria, está permitido formar $\{x : x \in A \text{ y } S(x)\}$, siendo este conjunto el mismo que $\{x \in A : S(x)\}$. Como ejemplos adicionales, podemos observar que

$$\{x: x \neq x\} = \varnothing$$

y

$$\{x: x = a\} = \{a\}.$$

En el caso en el que $S(x)$ es $(x \varepsilon' x)$, o en el caso en que es $(x = x)$, los "equis" especificados no constituyen un conjunto.

A pesar de la máxima de nunca obtener algo a partir de nada, parece ser un poco brusco que se diga que ciertos conjuntos no son realmente conjuntos y que ni siquiera debían ser mencionados sus nombres. Algunos tratamientos de la teoría de los conjuntos intentan suavizar este revés haciendo un uso sistemático de dichos conjuntos ilegales, pero sin llamarles conjuntos; la palabra acostumbrada es "clase". Una explicación precisa de lo que realmente son las clases y cómo se usan no viene al caso en el tratamiento presente. Hablando toscamente, una clase puede ser identificada con una condición (frase), o, más bien, con la "extensión" de una condición.

SECCION 4

UNIONES E INTERSECCIONES

Si A y B son conjuntos, a veces resulta natural el querer reunir sus elementos en un conjunto comprensivo.* Una manera de describir tal conjunto comprensivo es la de requerirle que contenga a todos los elementos que pertenezcan cuando menos a uno de los miembros de la pareja $\{A, B\}$. Esta formulación sugiere una generalización poderosa en sí misma; es seguro que una construcción similar podrá aplicarse a colecciones arbitrarias de conjuntos y no solamente a parejas de ellos. Lo que se quiere, en otras palabras, es el siguiente principio para la construcción de conjuntos:

> **Axioma de las uniones.** *Para toda colección de conjuntos existe un conjunto que contiene a todos los elementos que pertenecen cuando menos a uno de los conjuntos de la colección dada.*

Helo aquí nuevamente: para toda colección $\mathcal{C}$ existe un conjunto U tal que si $x \in X$ para algún X en $\mathcal{C}$, entonces $x \in U$. (Nótese que "cuando menos uno" significa lo mismo que "alguno").

El conjunto comprensivo U descrito anteriormente puede ser demasiado comprensivo, ya que puede contener elementos que no pertenezcan a ninguno de los conjuntos X de la colección $\mathcal{C}$. Sin embargo, esto es fácil de remediar, pues basta aplicar el axioma de la especificación para formar el conjunto

$$\{x \in U : x \in X \textit{ para algún } X \textit{ en } \mathcal{C}\}.$$

[Aquí la condición es una traducción al uso idiomático de la expresión más aceptable matemáticamente "*para algún X* (x

* Más usual es "incluyente" (N. del R.)

$\in X$ y $X \in \mathcal{C}$)."] De lo anterior se sigue que, para todo x, una condición necesaria y suficiente para que x pertenezca a este conjunto es que x pertenezca a X para algún X en $\mathcal{C}$. Si cambiamos notación y llamamos otra vez U al nuevo conjunto, entonces

$$U = \{x : x \in X \text{ para algún } X \text{ en } \mathcal{C}\}.$$

Este conjunto U es llamado la *unión* de la colección de conjuntos $\mathcal{C}$ y el axioma de la extensión garantiza que es único. El símbolo más simple para U que está en uso no es del todo muy popular en círculos matemáticos; éste es

$$\bigcup \mathcal{C}.$$

La mayoría de los matemáticos prefieren algo como

$$\bigcup \{X : X \in \mathcal{C}\}$$

o

$$\bigcup_{X \in \mathcal{C}} X.$$

En ciertos casos especiales importantes se dispone de otros recursos notacionales; serán descritos oportunamente.

Por el momento restringiremos nuestro estudio de la teoría de las uniones solamente a los hechos más simples. El más simple de todos es que

$$\bigcup \{X : X \in \varnothing\} = \varnothing,$$

y el que le sigue en simplicidad es que

$$\bigcup \{X : X \in \{A\}\} = A.$$

Con la notación brutalmente simple mencionada antes, estos hechos se expresan en la forma

$$\bigcup \varnothing = \varnothing$$

y

$$\bigcup \{A\} = A.$$

Las demostraciones son inmediatas a partir de las definiciones.

La unión de parejas de conjuntos es un poco más sustancial (después de todo, es lo que inició toda esta discusión). En este caso se usa una notación especial:

$$\bigcup \{X : X \in \{A, B\}\} = A \cup B.$$

La definición general de las uniones implica, en este caso especial, que $x \in A \cup B$ si y sólo si x pertenece a A, a B o a ambos, y se sigue que

$$A \cup B = \{x : x \in A \text{ o } x \in B\}.$$

He aquí algunos hechos fáciles de demostrar acerca de las uniones de parejas:

$$A \cup \varnothing = A,$$
$$A \cup B = B \cup A \text{ (conmutatividad)},$$
$$A \cup (B \cup C) = (A \cup B) \cup C \text{ (asociatividad)},$$
$$A \cup A = A \text{ (idempotencia)}$$
$$A \subset B \text{ si y sólo si } A \cup B = B.$$

Todo estudiante de matemáticas debe demostrar estos hechos para sí mismo cuando menos una vez en su vida. Las demostraciones están basadas en las propiedades elementales correspondientes del operador lógico *o*.

Un hecho igualmente simple, pero muy sugestivo es que

$$\{a\} \cup \{b\} = \{a, b\}.$$

Lo que esto sugiere es la forma de generalizar a las parejas. Concretamente, escribimos

$$\{a, b, c\} = \{a\} \cup \{b\} \cup \{c\}.$$

Esta ecuación define a su miembro de la izquierda. El miembro de la derecha debería incluir cuando menos una pareja de paréntesis, pero, en virtud de la ley de asociatividad su omisión no puede conducir a interpretaciones equivocadas. Ya que es fácil demostrar que

$$\{a, b, c\} = \{x : x = a \text{ o } x = b \text{ o } x = c\},$$

sabemos ahora que para cada tres conjuntos existe un conjunto que los contiene a ellos y nada más; resulta natural referirse a este conjunto, determinado, de manera única, como la *terna* (*no ordenada*) formada por dichos conjuntos. La extensión a mayor número de términos de la notación y terminología introducidas resulta obvia (*cuaternas*, etc).

La formación de uniones de conjuntos tiene muchos aspectos similares con otra operación de la teoría de los conjuntos. Si A y B son conjuntos, la *intersección* de A y B es el conjunto

$$A \cap B$$

definido en la forma

$$A \cap B = \{x \in A : x \in B\}.$$

La definición es simétrica en A y B a pesar de que parezca de otra manera; tenemos

$$A \cap B = \{x \in B : x \in A\},$$

y, de hecho, ya que $x \in A \cap B$ si y sólo si x pertenece tanto a A como a B, se sigue que

$$A \cap B = \{x : x \in A \text{ y } x \in B\}.$$

Los hechos básicos acerca de las intersecciones, así como sus demostraciones, son semejantes a los hechos básicos acerca de las uniones:

$$A \cap \varnothing = \varnothing,$$

$$A \cap B = B \cap A,$$

$$A \cap (B \cap C) = (A \cap B) \cap C,$$

$$A \cap A = A,$$

$$A \subset B \textit{ si y sólo si } A \cap B = A,$$

Parejas de conjuntos con intersección vacía se presentan con frecuencia suficiente como para justificar el uso de una palabra especial: si $A \cap B = \varnothing$, a los conjuntos A y B se les llama *ajenos*.* La misma palabra se aplica a veces a colecciones de conjuntos para indicar que dos conjuntos cualesquiera de la colección son ajenos; alternativamente, en tal situación hablaremos de una colección *de conjuntos ajenos*.

Dos hechos útiles acerca de uniones e intersecciones envuelven simultáneamente a las dos operaciones:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

A estas identidades se les llama *leyes distributivas*. Como ejemplo de una demostración en la teoría de conjuntos, demostraremos la segunda. Si x pertenece al primer miembro, entonces x pertenece, ya sea a A o a B y C; si x está en A, entonces x está tanto en $A \cup B$ como en $A \cup C$, y si x está en B y C, entonces, otra vez, x está tanto en $A \cup B$ como en $A \cup C$, y se sigue que, en cualquier caso, x pertenece al segundo miembro.

* La expresión no abreviada es *ajenos entre sí* o *mutuamente ajenos*. (N. del R.).

Esto muestra que el segundo miembro contiene al primero. Para demostrar que el primero contiene al segundo obérvese simplemente que si x pertenece tanto a $A \cup B$ como a $A \cup C$, entonces x pertenece, ya sea a A o a B y C.

La formación de la intersección de dos conjuntos A y B, o, como también podemos decir, la formación de la intersección de una pareja de conjuntos $\{A, B\}$, es un caso especial de una operación mucho más general. (Este es otro aspecto en el cual la teoría de las intersecciones se asemeja a la de las uniones): La existencia de la operación general de la intersección depende del hecho de que para cada colección no vacía, de conjuntos existe un conjunto que contiene exactamente a aquellos elementos que pertenecen a cada conjunto de la colección dada. En otras palabras: para cada colección $\mathcal{C}$, distinta de $\varnothing$, existe un conjunto V tal que $x \in V$ si y sólo si $x \in X$ para cada X en $\mathcal{C}$. Para demostrar esta aseveración, sea A cualquier conjunto particular en $\mathcal{C}$ (este paso está justificado por el hecho de que $\mathcal{C} \neq \varnothing$) y escríbase

$$V = \{x \in A : x \in X \textit{ para cada } X \textit{ en } \mathcal{C}\}.$$

[La condición significa "*para todo* X (*si* X $\in \mathcal{C}$, *entonces* $x \in X$)."] La dependencia de V de la elección arbitraria de A es ilusoria; de hecho

$$V = \{x : x \in X \textit{ para cada } X \textit{ en } \mathcal{C}\}.$$

Al conjunto V se le conoce como la *intersección* de la colección de conjuntos $\mathcal{C}$; el axioma de la extensión garantiza su unicidad. La notación acostumbrada es semejante a la de las uniones: en lugar del inobjetable pero impopular

$$\bigcap \mathcal{C},$$

el conjunto V es denotado usualmente en la forma

$$\bigcap \{X : X \in \mathcal{C}\}$$

o

$$\bigcap\nolimits_{X \in \mathcal{C}} X.$$

EJERCICIO. Una condición necesaria y suficiente para que $(A \cap B) \cup C = A \cap (B \cup C)$ es que $C \subset A$. Obsérvese que la condición no tiene nada que ver con el conjunto B.

SECCION 5

COMPLEMENTOS Y POTENCIAS

Si A y B son conjuntos, la *diferencia entre* A y B, más frecuentemente conocida como el *complemento relativo* de B respecto a A, es el conjunto $A - B$ definido en la forma

$$A - B = \{x \in A : x \notin B\}.$$

Nótese que en esta definición no es necesario suponer que $B \subset A$. Sin embargo, con el fin de registrar los hechos básicos acerca de la complementación tan simplemente como sea posible, supondremos (sólo en esta sección) que todos los conjuntos que se mencionen son subconjuntos de un mismo conjunto E, y que todos los complementos (a menos que se especifique otra cosa), se forman con respecto a E. En tales condiciones (que son muy frecuentes) es más fácil recordar el conjunto fundamental E que continuar escribiéndolo, lo cual permite simplificar la notación. Un símbolo que se usa a menudo para denotar el complemento, temporalmente absoluto, (en oposición a relativo) de A es A'. En términos de este símbolo, los hechos básicos acerca de la complementación pueden ser establecidos en la forma siguiente:

$$(A')' = A,$$

$$\varnothing' = E, \quad E' = \varnothing,$$

$$A \cap A' = \varnothing, \quad A \cup A' = E,$$

$$A \subset B \text{ si y sólo si } B' \subset A'$$

Los enunciados más importantes acerca de complementos son las llamadas *leyes de De Morgan*:

$$(A \cup B)' = A' \cap B', \quad (A \cap B)' = A' \cup B'.$$

(Veremos en seguida que las leyes de De Morgan se cumplen para las uniones y las intersecciones de colecciones más grandes de conjuntos y no solamente para las parejas). Estos hechos acerca de la complementación implican que, en la teoría de los conjuntos, los teoremas se presentan usualmente por pares. Si en una inclusión o ecuación concerniente a uniones, intersecciones y complementos de subconjuntos de E, reemplazamos cada conjunto por su complemento, intercambiamos uniones e intersecciones e invertimos todas las inclusiones, el resultado es otro teorema. Este hecho se conoce a veces como el *principio de la dualidad* para conjuntos.

He aquí algunos ejercicios sencillos sobre complementación

$$A - B = A \cap B'.$$

$$A \subset B \text{ si y sólo si } A - B = \varnothing.$$

$$A - (A - B) = A \cap B.$$

$$A \cap (B - C) = (A \cap B) - (A \cap C).$$

$$A \cap B \subset (A \cap C) \cup (B \cap C').$$

$$(A \cup C) \cap (B \cup C') \subset A \cup B.$$

Si A y B son conjuntos, la *diferencia simétrica* (*o suma Booleana*) de A y B es el conjunto $A + B$ definido en la forma

$$A + B = (A - B) \cup (B - A).$$

Esta operación es conmutativa ($A + B = B + A$), asociativa ($A + (B + C) = (A + B) + C$) y tal que $A + \varnothing = A$ y $A + A = \varnothing$.

Este puede ser el momento oportuno para aclarar una parte trivial, pero ocasionalmente confusa de la teoría de las intersecciones. Para comenzar, recúerdese que las intersecciones fueron definidas solamente para colecciones no vacías. La razón es que el mismo proceso aplicado a la colección vacía no define un conjunto. ¿Cuáles "equis" están especificados por la frase

$$x \in X \text{ para cada } X \text{ en } \varnothing?$$

Como es usual para preguntas acerca de $\varnothing$, la respuesta se ve más fácilmente a partir de la pregunta contraria. ¿Cuáles "equis" *no* satisfacen la condición propuesta? Si no es cierto que $x \in X$ para cada X en $\varnothing$, deberá existir entonces algún X

en $\varnothing$ tal que $x \epsilon' X$; pero, como no existe ningún X en $\varnothing$, esto es absurdo. Conclusión: ningún x deja de satisfacer la condición propuesta, o, lo que es lo mismo, todo x la satisface. En otras palabras, los "equis" especificados por la condición agotan al universo (inexistente). No hay aquí ningún problema profundo. Es tan sólo una molestia el estár siempre forzado a hacer distinciones y excepciones sólo porque algún conjunto en alguna parte a lo largo de alguna construcción puede resultar vacío. No hay nada que hacer al respecto; es, simplemente, un hecho de la vida.

Si limitamos nuestra atención a subconjuntos de un conjunto particular E, como hemos acordado temporalmente, entonces la molestia descrita en el párrafo anterior parece alejarse. El hecho es que, en este caso, la intersección de una colección $\mathcal{C}$ (de subconjuntos de E) podemos definirla como el conjunto

$$\{x \epsilon E : x \epsilon X \text{ para cada } X \text{ en } \mathcal{C}\}.$$

Esto no es nada revolucionario; para cada colección no vacía, la nueva definición concuerda con la original. La diferencia está en la forma en que una y otra tratan a la colección vacía; de acuerdo con la nueva definición $\bigcap_{X \epsilon \varnothing} X$ es igual a E. (¿Para qué elementos x de E puede ser falso que $x \epsilon X$ para cada X en $\varnothing$?) la diferencia es sólo una cuestión de lenguaje. Una ligera meditación revela que la "nueva" definición propuesta para la intersección de una colección $\mathcal{C}$ de subconjuntos de E es de hecho lo mismo que la definición original de la intersección de la colección $\mathcal{C} \cup \{E\}$, y esta última nunca es vacía.

Hemos estado considerando los subconjuntos de un conjunto E; ¿constituyen estos subconjuntos por sí solos un conjunto? El siguiente principio garantiza que la respuesta es afirmativa.

Axioma de las potencias. *Para cada conjunto existe una colección de conjuntos que contiene entre sus elementos a todos los subconjuntos del conjunto dado.*

En otras palabras, si E es un conjunto, entonces existe un conjunto (colección) $\mathcal{P}$ tal que si $X \subset E$, entonces $X \epsilon \mathcal{P}$.

El conjunto $\mathcal{P}$ descrito anteriormente puede ser más extenso de lo deseado, ya que puede contener otros elementos además de los subconjuntos de E. Esto se remedia fácilmente; basta aplicar el axioma de la especificación para formar el

conjunto $\{X \in \mathcal{P} : X \subset E\}$. [Recuérdese que "$X \subset E$" expresa lo mismo que "*para todo* x (*si* $x \in X$ *entonces* $x \in E$)"]. Ya que, para cada X, una condición necesaria y suficiente para que X pertenezca a este conjunto es que X sea un subconjunto de E, se sigue que si cambiamos notación y llamamos otra vez $\mathcal{P}$ a este conjunto, entonces

$$\mathcal{P} = \{X : X \subset E\}.$$

Al conjunto $\mathcal{P}$ se le llama *conjunto potencia* de E y el axioma de la extensión garantiza que es único. El hecho de que $\mathcal{P}$ depende de E se denota escribiendo $\mathcal{P}(E)$ en lugar de escribir solamente $\mathcal{P}$.

Como el conjunto $\mathcal{P}(E)$ es muy grande en comparación con E. no es fácil dar ejemplos. Si $E = \varnothing$, la situación es bastante clara: el conjunto $\mathcal{P}(E)$ es el conjunto singular $\{\varnothing\}$. Los conjuntos potencia de conjuntos singulares y de parejas son también fácilmente descriptibles: tenemos

$$\mathcal{P}(\{a\}) = \{\varnothing, \{a\}\}$$

y

$$\mathcal{P}(\{a, b\}) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}.$$

El conjunto potencia de una terna tiene ocho elementos. El lector imagina probablemente (y por ello está retado a demostrar) la generalización que incluye a todos los enunciados anteriores: el conjunto potencia de un conjunto finito de, digamos *n elementos*, tiene 2^n elementos. (Por supuesto, conceptos como "finito" y "2^n" no tienen aún categoría oficial para nosotros; pero ello no impide que sean comprendidos en forma no oficial).

La ocurrencia de n como exponente (la enésima potencia de 2) tiene algo que ver con la razón por la cual un conjunto potencia lleva ese nombre.

Si $\mathcal{C}$ es una colección de subconjuntos de un conjunto E [esto es, que $\mathcal{C}$ es una subcolección de $\mathcal{P}(E)$], entonces escriba

$$\mathcal{D} = \{X \in \mathcal{P}(E) : X' \in \mathcal{C}\}.$$

(Para tener la certeza de que la condición usada en la definición de $\mathcal{D}$ es una frase en el sentido técnico preciso, debe reescribirse en una forma por el estilo de la siguiente:

Para algún Y [$Y \in \mathcal{C}$ *y para todo* x ($x \in X$ *si y sólo si* ($x \in E$ *y* $x \in' Y$))].

Observaciones semejantes se hacen frecuentemente cuando queremos usar abreviaturas definidas en vez de usar solamente primitivos lógicos y de la teoría de los conjuntos. La traducción rara vez exige ingeniosidad y usualmente la omitiremos). Es costumbre denotar la unión y la intersección de la colección $\mathfrak{D}$ por los símbolos.

$$\bigcup_{X \in \mathcal{C}} X' \quad \text{y} \quad \bigcap_{X \in \mathcal{C}} X'.$$

Con esta notación, las expresiones generales de las leyes de De Morgan pasan a ser

$$\left(\bigcup_{X \in \mathcal{C}} X\right)' = \bigcap_{X \in \mathcal{C}} X'$$

y

$$\left(\bigcap_{X \in \mathcal{C}} X\right)' = \bigcup_{X \in \mathcal{C}} X'.$$

Las demostraciones de estas ecuaciones son consecuencias inmediatas de las definiciones apropiadas

EJERCICIO. Demuestre que $\mathcal{P}(E) \cap \mathcal{P}(F) = \mathcal{P}(E \cap F)$ y que $\mathcal{P}(E) \cup \mathcal{P}(F) \subset \mathcal{P}(E \cup F)$. Estas aseveraciones pueden generalizarse a

$$\bigcap_{X \in \mathcal{C}} \mathcal{P}(X) = \mathcal{P}\left(\bigcap_{X \in \mathcal{C}} X\right)$$

y

$$\bigcup_{X \in \mathcal{C}} \mathcal{P}(X) \subset \mathcal{P}\left(\bigcup_{X \in \mathcal{C}} X\right);$$

encuentre una interpretación razonable de la notación en la que fueron expresadas estas generalizaciones y entonces demuéstrelas. Otros hechos elementales son:

$$\bigcap_{X \in \mathcal{P}(E)} X = \varnothing,$$

y

$$\textit{si } E \subset F, \text{ entonces } \mathcal{P}(E) \subset \mathcal{P}(F)$$

Una cuestión curiosa tiene que ver con la conmutatividad de los operadores $\mathcal{P}$ y $\bigcup$. Haga ver que E es siempre igual a $\bigcup_{X \in \mathcal{P}(E)} X$ [esto es, $E = \bigcup \mathcal{P}(E)$], pero que el resultado de aplicar $\mathcal{P}$ y $\bigcup$ a E en el orden inverso es un conjunto que incluye a E como un subconjunto propio.

SECCION 6

PAREJAS ORDENADAS

¿Qué significa arreglar los elementos de un conjunto A en algún orden? Supóngase, por ejemplo, que el conjunto A es la cuaterna $\{a, b, c, d\}$ de elementos distintos entre sí y que queremos considerarlos en el orden

$$c\ b\ d\ a.$$

Aún sin una definición precisa de lo que esto significa, podemos hacer con ellos algo que es sensato en teoría de conjuntos. A saber, podemos considerar, para cada posición particular en la ordenación, el conjunto de todos aquellos elementos que se presenten en dicha posición o delante de ella, obteniendo así los conjuntos

$$\{c\} \quad \{c, b\} \quad \{c, b, d\} \quad \{c, b, d, a\}.$$

Podemos seguir adelante considerando luego el conjunto (o colección, si así suena mejor)

$$\mathcal{C} = \{\{a, b, c, d\}, \{b, c\}, \{b, c, d\}, \{c\}\}$$

cuyos elementos son precisamente esos conjuntos. Con el fin de recalcar que el concepto de orden, apoyado en la intuición y quizás poco claro, ha logrado producir algo sólido y simple, a saber, un conjunto $\mathcal{C}$ llano y sin adornos, los elementos de $\mathcal{C}$ y *sus* elementos han sido presentados anteriormente en forma desordenada. (El lector lexicográficamente propenso debe ser capaz de encontrar un método en la manera de revolverlos.)

Sigamos pretendiendo por un tiempo que sabemos lo que significa orden. Supóngase que en una rápida ojeada al párrafo precedente todo lo que pudimos captar es el conjunto $\mathcal{C}$; ¿po-

demos valernos de él para recuperar el orden que le dió origen? Se ve fácilmente que la respuesta es afirmativa. Examine los elementos de $\mathcal{C}$ (ellos en sí mismos son conjuntos, por supuesto) para encontrar uno que esté incluido en todos los demás; como $\{c\}$ cumple el requisito (y ningún otro lo hace) sabemos que c debió ser el primer elemento. Busque a continuación el siguiente elemento más pequeño de $\mathcal{C}$, esto es, aquel que está incluido en todos los que quedan después de eliminar a $\{c\}$; como $\{b, c\}$ llena el requisito (y ningún otro lo hace) sabemos que b debió ser el segundo elemento. Procediendo de esta manera (sólo hacen falta dos pasos más) podemos pasar del conjunto $\mathcal{C}$ al orden dado del conjunto dado A.

La moraleja es ésta: quizá no sepamos precisamente lo que significa ordenar los elementos de un conjunto A, pero con cada orden podemos asociar un conjunto $\mathcal{C}$ de subconjuntos de A de tal manera que el orden dado puede recuperarse a partir de $\mathcal{C}$ y es el único orden con tal propiedad. (He aquí un ejercicio no trivial: encuentre una caracterización intrínseca de aquellos conjuntos de subconjuntos de A que correspondan a algún orden en A. Ya que "orden" todavía no tiene significado oficial para nosotros, el problema entero carece de significado oficial. Nada de lo que sigue depende de su solución pero el lector aprenderá algo de valor al tratar de encontrarla). El paso de un orden en A al conjunto $\mathcal{C}$, y viceversa, fue ilustrado anteriormente para una cuaterna; para una pareja todo pasa a ser, cuando menos, doblemente simple Si $A = \{a, b\}$ y, si en el orden deseado, a viene primero, entonces $\mathcal{C} = \{\{a\}, \{a, b\}\}$; si, en cambio, b viene primero entonces $\mathcal{C} = \{\{b\}, \{a, b\}\}$.

La *pareja ordenada* de a y b, con *primera coordenada* a y *segunda coordenada* b, es el conjunto (a, b) definido en la forma

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Por muy convincente que pueda ser la motivación de esta definición, aún debemos probar que el resultado tiene la propiedad principal de que una pareja ordenada tiene que merecer su nombre. Debemos hacer ver que si (a, b) y (x, y) son parejas ordenadas y $(a, b) = (x, y)$, entonces $a = x$ y $b = y$. Para demostrar esto, observemos primero que si a y b son iguales, entonces la pareja ordenada (a, b) es lo mismo que el conjunto singular $\{\{a\}\}$. Si, recíprocamente, (a, b) es un conjunto sin-

gular, entonces $\{a\} = \{a, b\}$, de manera que $b \in \{a\}$, y, por lo tanto, $a = b$. Supóngase ahora que $(a, b) = (x, y)$. Si $a = b$, entonces tanto (a, b) como (x, y) son conjuntos singulares, de manera que $x = y$ y ya que $\{x\} \in (a, b)$ y $\{a\} \in (x, y)$, se sigue que a, b, x, y y son todos iguales. Si $a \neq b$, entonces tanto (a, b) como (x, y) contienen exactamente un conjunto singular, a saber, $\{a\}$ y $\{x\}$, respectivamente, de manera que $a = x$. Como en este caso es también cierto que ambos (a, b) y (x, y) contienen exactamente una pareja no ordenada, a saber, $\{a, b\}$ y $\{x, y\}$, respectivamente, se sigue que $\{a, b\} = \{x, y\}$ y, por lo tanto, en particular, $b \in \{x, y\}$. Como b no puede ser x (ya que entonces tendríamos $a = x$, $b = x$ y, por lo tanto, $a = b$), deberá tenerse $b = y$, lo cual completa la demostración.

Si A y B son conjuntos ¿existe un conjunto que contiene a todas las parejas ordenadas (a, b) con a en A y b en B? Es bastante fácil ver que la respuesta es afirmativa. En efecto, si $a \in A$ y $b \in B$, entonces $\{a\} \subset A$ y $\{b\} \subset B$, y por lo tanto $\{a, b\} \subset A \cup B$. Como también $\{a\} \subset A \cup B$, se sigue que ambos $\{a\}$ y $\{a, b\}$ son elementos de $\mathcal{P}(A \cup B)$. Esto implica que $\{\{a\}, \{a, b\}\}$ es un subconjunto de $\mathcal{P}(A \cup B)$, y con ello, que es un elemento de $\mathcal{P}[\mathcal{P}(A \cup B)]$; en otras palabras, $(a, b) \in \mathcal{P}[\mathcal{P}(A \cup B)]$ siempre que $a \in A$ y $b \in B$. Una vez que esto es sabido, es cuestión de rutina aplicar el axioma de la especificación y el axioma de la extensión para producir el conjunto único $A \times B$ que está constituido precisamente por las parejas ordenadas (a, b) con a en A y b en B. A este conjunto se le llama *producto cartesiano* de A y B y está caracterizado por el hecho de que

$$A \times B = \{x : x = (a, b) \textit{ para algún } a \textit{ en } A \textit{ y algún } b \textit{ en } B\}.$$

El producto cartesiano de dos conjuntos es un conjunto de parejas ordenadas (esto es, un conjunto cuyos elementos son, cada uno, una pareja ordenada), y lo mismo sucede con todo subconjunto de un producto cartesiano. Es de importancia técnica saber que podemos seguir también el camino recíproco: todo conjunto de parejas ordenadas es un subconjunto del producto cartesiano de dos conjuntos. En otras palabras: si R es un conjunto tal que todo elemento de R es una pareja ordenada, entonces existen dos conjuntos A y B tales que $R \subset A \times B$. La demostración es elemental. En efecto, supóngase que $x \in R$ de manera que $x = \{\{a\}, \{a, b\}\}$ para algún a y

para algún b. El problema es el de sacar a a y b de las llaves. Ya que los elementos de R son conjuntos, podemos formar la unión de los conjuntos de R; como x es uno de los conjuntos de R, los elementos de x pertenecen a esa unión. Como $\{a, b\}$ es uno de los elementos de x, podemos escribir en la forma descrita anteriormente como la notación brutal, $\{a, b\} \in \bigcup R$. Un juego de llaves ha desaparecido; hagamos otra vez la misma cosa para que desaparezca el otro. Fórmese la unión de los conjuntos de $\bigcup R$. Como $\{a, b\}$ es uno de esos conjuntos, se sigue que los elementos de $\{a, b\}$ pertenecen a esa unión y, por lo tanto, a y b pertenecen a $\bigcup\bigcup R$. Esto alcanza el objetivo señalado anteriormente; para exhibir a R como subconjunto de algún $A \times B$, debemos tomar a ambos A y B como $\bigcup\bigcup R$. Es a menudo deseable tomar a A y a B tan chicos como sea posible. Para lograrlo, basta aplicar el axioma de la especificación para formar los conjuntos

$$A = \{a: \textit{para algún } b\ [(a, b) \in R]\}$$

y

$$B = \{b: \textit{para algún } a\ [(a, b) \in R]\}.$$

A estos conjuntos se les conoce como las *proyecciones* de R sobre la primera y segunda coordenada, respectivamente.

Por muy importante que sea ahora la teoría de los conjuntos, cuando comenzó, algunos eruditos la consideraron como una enfermedad de la cual era deseable que las matemáticas se recobrasen pronto. Por esta razón, muchas consideraciones de la teoría de los conjuntos fueron llamadas patológicas y la palabra se incorporó al lenguaje del matemático aplicándose frecuentemente a algo que no agrada a un interlocutor. La definición explícita de una pareja ordenada $[(a, b) = \{\{a\}, \{a, b\}\}]$ es relegada frecuentemente a la teoría de conjuntos patológica. En pro de aquellos que consideran que en este caso el nombre es merecido, hacemos notar que la definición ha llenado su cometido por ahora y no se volverá a usar más. Necesitamos saber que las parejas ordenadas son determinadas por y determinan en forma única su primera y segunda coordenadas, que pueden formarse productos cartesianos y que todo conjunto de parejas ordenadas es un subconjunto de algún producto cartesiano; la vía de entrada particular empleada para lograr estos propósitos carece de importancia.

Es fácil localizar la fuente de la desconfianza y recelo que sienten muchos matemáticos hacia la definición explícita de pareja ordenada expuesta anteriormente. El problema no es que algo esté mal o que algo falte; todas las propiedades pertinentes del concepto que hemos definido son correctas (esto es, acordes con las exigencias de la intuición) y todas las propiedades correctas están presentes. El problema es que el concepto tiene algunas propiedades que no vienen al caso, que son accidentales y distraen. El teorema de que $(a, b) = (x, y)$ si y sólo si $a = x$ y $b = y$ es la clase de hecho que esperamos aprender acerca de las parejas ordenadas. Por otra parte, el hecho de que $\{a, b\} \in (a, b)$ parece accidental; es una propiedad caprichosa de la definición más que una propiedad intrínseca del concepto.

La carga de artificialidad es verdadera, pero no constituye un precio demasiado alto para la economía conceptual. El concepto de pareja ordenada puede ser introducido como un primitivo adicional, axiomáticamente dotado con las propiedades convenientes, ni una más ni una menos. En algunas teorías se hace así. La alternativa del matemático está entre tener que recordar unos cuantos axiomas más y tener que olvidar unos cuantos hechos accidentales; es bien claro que la elección es cuestión de gustos. Elecciones semejantes tienen lugar frecuentemente en matemáticas; en este libro, por ejemplo, las encontraremos otra vez en relación a las definiciones de números de varios tipos.

EJERCICIO. Si A, B, X y Y son conjuntos, entonces

(i) $(A \cup B) \times X = (A \times X) \cup (B \times X)$,

(ii) $(A \cap B) \times (X \cap Y) = (A \times X) \cap (B \times Y)$,

(iii) $(A - B) \times X = (A \times X) - (B \times X)$.

Si $A = \varnothing$ o $B = \varnothing$, entonces $A \times B = \varnothing$, y recíprocamente. Si $A \subset X$ y $B \subset Y$, entonces $A \times B \subset X \times Y$, y recíprocamente (siempre que $A \times B \neq \varnothing$).

SECCION 7

RELACIONES

Empleando parejas ordenadas, podemos formular la teoría matemática de las relaciones en el lenguaje de la teoría de conjuntos. Por relación entendemos aquí algo como matrimonio (entre hombres y mujeres) o pertenencia (entre elementos y conjuntos). Más explícitamente, lo que llamaremos relación es conocido a veces como relación *binaria*. Un ejemplo de relación ternaria es el de la paternidad en la gente (Adán y Eva son los padres de Caín). En este libro no tendremos ocasión de estudiar la teoría de las relaciones que son ternarias, cuaternarias o peores.

Dirigiendo la atención hacia cualquier relación específica, tal como el matrimonio por ejemplo, podríamos estar tentados a considerar ciertas parejas ordenadas (x, y), a saber, justamente aquellas en las cuales x es un hombre, y es una mujer y x está casado con y. No hemos visto aún la definición del concepto general de una relación, pero parece factible que, tal como en este ejemplo del matrimonio, toda relación debe determinar de manera única al conjunto de todas aquellas parejas ordenadas, en las cuales la primera coordenada mantiene esta relación con la segunda. Si conocemos la relación, conocemos el conjunto y, mejor aún, si conocemos el conjunto, conocemos la relación. Si por ejemplo, fuéramos presentados con el conjunto de parejas ordenadas de gente que corresponde al matrimonio, entonces, aun si olvidáramos la definición de matrimonio, podríamos decir siempre cuándo un hombre x está casado con una mujer y y cuando no; sólo tendríamos que ver si la pareja ordenada (x, y) pertenece al conjunto o no.

Quizá no sepamos lo que es una relación, pero sabemos lo que es un conjunto y las consideraciones precedentes establecen una estrecha conexión entre relaciones y conjuntos. El estudio preciso de las relaciones en la teoría de los conjuntos saca provecho de esta conexión heurística; lo más fácil de hacer es definir una relación como el conjunto correspondiente. Esto es lo que hacemos; definimos por este medio una *relación* como un conjunto de parejas ordenadas. Explícitamente: Un conjunto R es una relación si cada elemento de R es una pareja ordenada; esto significa, por supuesto, que si $z \in R$ entonces existen x y y de manera que $z = (x, y)$. Si R es una relación, es conveniente a veces expresar el hecho de que $(x, y) \in R$ escribiendo

$$x R y$$

y diciendo, como en el lenguaje ordinario, que x está en la relación R con y.

La relación menos excitante es la vacía. (Para demostrar que $\varnothing$ es un conjunto de parejas ordenadas, busque un elemento de $\varnothing$ que no sea una pareja ordenada.) Otro ejemplo soso es el producto cartesiano de dos conjuntos X y Y. He aquí un ejemplo ligeramente más interesante: sea X un conjunto cualquiera y sea R el conjunto de todas aquellas parejas (x, y) de $X \times X$ para las cuales $x = y$. La relación R es precisamente la relación de igualdad entre elementos de X; si x y y están en X, entonces $x \; R \; y$ significa lo mismo que $x = y$. Un ejemplo más será suficiente por ahora: sea X cualquier conjunto y sea R el conjunto de todas aquellas parejas (x, A) de $X \times \mathcal{P}(X)$ para las cuales $x \in A$. Esta relación R es justamente la de pertenencia entre elementos de X y subconjuntos de X; si $x \in X$ y $A \in \mathcal{P}(X)$, entonces $x \; R \; A$ significa lo mismo que $x \in A$.

En la sección precedente vimos que a cada conjunto R de parejas ordenadas están asociados dos conjuntos conocidos como las proyecciones de R sobre la primera y segunda coordenadas. En la teoría de las relaciones estos conjuntos son conocidos como el *dominio* y el *rango* de R (abreviándose dom R y ran R). Recalcamos que ellos están definidos en la forma

$$\text{dom } R = \{x\colon \textit{para algún } y \; (x \; R \; y)\}$$

y

$$\text{ran } R = \{y\colon \textit{para algún } x \; (x \; R \; y)\}.$$

Si R es la relación matrimonio, de manera que $x \; R \; y$ signifique que x es un hombre, y una mujer y que x y y están casados el uno con la otra, entonces dom R es el conjunto de los hombres casados y ran R el conjunto de las mujeres casadas. Tanto el dominio como el rango de $\varnothing$ son iguales a $\varnothing$. Si $R = X \times Y$ entonces dom $R = X$ y ran $R = Y$. Si R es igualdad en X, entonces dom R = ran $R = X$. Si R es pertenencia entre X y $\mathcal{P}(X)$, entonces dom $R =$ y ran $R = \mathcal{P}(X) - \{\varnothing\}$.

Si R es una relación incluida en un producto cartesiano $X \times Y$ (de manera que dom $R \subset X$ y ran $R \subset Y$), a veces es conveniente decir que R es una relación *de* X *a* Y; en vez de una relación de X a X podemos hablar de una relación *en* X. Una relación R en X es *reflexiva* si $x \; R \; x$ para todo x de X; es *simétrica* si $x \; R \; y$ implica $y \; R \; x$; y es *transitiva* si $x \; R \; y$ y $y \; R \; z$ implican que $x \; R \; z$. (Ejercicio: para cada una de estas tres propiedades posibles encuentre una relación que no tenga esa propiedad pero que sí tenga las otras dos.) Una relación en un conjunto es una *relación de equivalencia* si es reflexiva, simétrica y transitiva. La relación de equivalencia más chica en un conjunto X es la relación de igualdad en X, y la más grande es $X \times X$.

Hay una conexión íntima entre las relaciones de equivalencia en un conjunto X y ciertas colecciones (llamadas particiones) de subconjuntos de X. Una *partición de* X es una colección $\mathcal{C}$ de subconjuntos no vacíos y ajenos entre sí, de X, cuya unión es X. Si R es una relación de equivalencia en X y si x está en X la *clase de equivalencia* de x respecto a R es el conjuto de todos aquellos elementos y de X para los cuales $x \; R \; y$. (El peso de la tradición hace inevitable el uso de la palabra "clase" en este caso.) Ejemplos: si R es igualdad en X, entonces cada clase de equivalencia es un cojunto singular* si $R = X \times X$, entonces el conjunto X mismo es la única clase de equivalencia. No hay una notación única para la clase de equivalencia de x respecto a R; usualmente la denotaremos por x/R y escribiremos X/R para representar el conjunto de todas las clases de equivalencia [Lea X/R diciendo "X módulo R". Ejercicio: haga ver que X/R es de hecho un conjunto, exhibiendo una condición que especifique exactamente al subconjunto X/R del conjunto potencia $\mathcal{P}(X)$.] Ahora, olvide a R por un tiempo y

* Véase pág. 19.

comience nuevamente con una partición $\mathcal{C}$ de X. Una relación, a la cual llamaremos $X/\mathcal{C}$, está definida en X escribiendo

$$x \; X/\mathcal{C} \; y$$

sólo en el caso en que x y y pertenecen al mismo conjunto de la colección $\mathcal{C}$. Llamaremos $X/\mathcal{C}$ a la relación *inducida* por la partición $\mathcal{C}$.

En el párrafo precedente vimos cómo asociar un conjunto de subconjuntos de X con cada relación de equivalencia en X, y cómo asociar una relación en X con cada partición de X. La conexión entre relaciónes de equivalencia y particiones puede ser descrita diciendo que el paso de $\mathcal{C}$ a $X/\mathcal{C}$ es exactamente el contrario del paso de R a X/R. Más explícitamente: si R es una relación de equivalencia en X, entonces el conjunto de las clases de equivalencia es una partición de X que induce la relación R, y si $\mathcal{C}$ es una partición de X, entonces la relación inducida es una relación de equivalencia cuyo conjunto de clases de equivalencia es precisamente $\mathcal{C}$.

Para demostrarlo, comencemos con una relación de equivalencia R. Como cada x pertenece a una clase de equivalencia (por ejemplo, $x \in x/R$) es claro que la unión de todas las clases de equivalencia es todo el conjunto X. Si $z \in x/R \cap y/R$, entonces $x \, R \, z$ y $z \, R \, y$, y por lo tanto, $x \, R \, y$. Esto implica que si dos clases de equivalencia tienen un elemento común, son idénticas entre sí, o, en otras palabras, que dos clases de equivalencia distintas entre sí, son siempre ajenas. Así, el conjunto de las clases de equivalencia es una partición. Decir que dos elementos pertenecen al mismo conjunto (clase de equivalencia) de esta partición significa por definición, que están en la relación R uno con otro. Esto demuestra la primera mitad de nuestra proposición.

La segunda mitad es más sencilla. Comiéncese con una partición $\mathcal{C}$ y considérese la relación inducida. Ya que todo elemento de X pertenece a algún conjunto de $\mathcal{C}$, la reflexividad establece simplemente que x y x están en el mismo conjunto de $\mathcal{C}$. La simetría dice que si x y y están en el mismo conjunto de $\mathcal{C}$, entonces y y x están en el mismo conjunto de $\mathcal{C}$, lo cual es obviamente cierto. La transitividad afirma que si x y y están en el mismo conjunto de $\mathcal{C}$ a la vez que

y y z están en el mismo conjunto de $\mathcal{C}$, entonces x y z están en el mismo conjunto de $\mathcal{C}$, lo cual es obvio también. La clase de equivalencia de cada x de X es precisamente el conjunto $\mathcal{C}$ al cual pertenece x. Esto completa la demostración de todo lo que se propuso.

SECCION 8

FUNCIONES

Si X y Y son conjuntos, una *función* de (o *en*) X *a* (o *en*) Y** es una relación f tal que dom $f = X$ y tal que para cada x de X existe un solo elemento y en Y con $(x, y) \in f$. La condición de que el elemento de Y debe ser único puede formularse explícitamente como sigue: si $(x, y) \in f$ y $(x, z) \in f$, entonces $y = z$. Para cada x de X, el único y de Y tal que $(x, y) \in f$ se denota por $f(x)$. Para funciones, esta notación y sus pequeñas variantes reemplaza a otras que se usan para relaciones más generales; de aquí en adelante, si f es una función escribiremos $f(x) = y$ en vez de $(x, y) \in f$ o $x\ f\ y$. El elemento y es conocido como el *valor* que la función f *asume* (o *toma*) para el *argumento* x; podemos decir también que f *envía* x hacia y, que *mapea* a x sobre y o que *transforma* a x en y. Las palabras *mapeo*, *transformación*, *correspondencia* y *operador*, están entre las muchas que se usan a veces como sinónimo de *función*. El símbolo

$$f: X \to Y$$

se usa a veces como abreviatura de "f es una función de X a Y". El conjunto de todas las funciones de X a Y es un subconjunto del conjunto potencia $\mathcal{P}(X \times Y)$ y será denotado por Y^X

Las connotaciones de actividad sugeridas por los sinónimos anotados anteriormente hacen que algunos eruditos queden insatisfechos con la definición de acuerdo con la cual, una función no *hace* nada sino que simplemente es. Esta insatisfacción se refleja en un diferente uso del vocabulario: *función* se reserva para el objeto indefinido que de alguna manera

* Mapear, término puramente técnico tiene un uso muy restringido. (N. del R.).

** En el original "f on X" nos dice que f está definida en X que es el dominio; "f into Y" dice que f tiene contradominio Y. El "*on*" y el "*into*" se traducen frecuentemente como "en" pero esto no es inconveniente si se acuerda que: "f en X" o "f de X" dicen que X es dominio y "f de X en Y" dice que Y es contradominio (N. del R.)

está activo, y el conjunto de parejas ordenadas que hemos llamado función es conocido entonces como la *gráfica* de la función. Es fácil encontrar ejemplos de funciones en el preciso sentido de la palabra que da la teoría de los conjuntos, tanto en matemáticas como en la vida diaria. Todo lo que tenemos que buscar es información, no necesariamente numérica, en forma tabulada. Un ejemplo es el directorio de una ciudad; en este caso, los argumentos de la función son los habitantes de la ciudad, y los valores son sus direcciones.

Hemos definido los conceptos de dominio y rango para relaciones en general y, por lo tanto, en particular, para funciones. El dominio de una función f de X a Y es, por definición, igual a X, pero su rango no tiene que ser igual a Y; el rango está constituido por aquellos elementos y de Y para los cuales existe un x en X tal que $f(x) = y$. Si el rango de f es igual a Y decimos que f transforma a X *sobre* Y. Si A es un subconjunto de X, es posible que nos interese considerar el conjunto de todos aquellos elementos y de Y para los cuales existe x en el subconjunto A tal que $f(x) = y$. A este subconjunto de Y se le conoce como la *imagen* de A bajo f y frecuentemente es denotado por $f(A)$. La notación es mala pero no catastrófica. Lo malo de ella es que si A resulta ser un elemento de X a la vez que un subconjunto de X (una situación improbable, pero muy lejos de ser imposible), entonces el símbolo $f(A)$ presenta una ambigüedad. ¿Significa el valor de f correspondiente a A o representa al conjunto de valores de f correspondientes a los elementos de A? Siguiendo la costumbre usual de las matemáticas, usaremos la mala notación, apoyándonos en el contexto y, en las raras ocasiones en que se haga necesario, agregando estipulaciones verbales para eliminar la confusión. Nótese que la imagen de X es el rango de f; el carácter "sobre" de f puede expresarse escribiendo $f(X) = Y$.

Si X es un subconjunto de un conjunto Y, la función f definida por $f(x) = x$ para cada x de X es conocida como la *inclusión* (o el *encaje*, o la *inyección*) de X en Y. La frase "la función f definida por..." es muy común. Por supuesto, se está implicando que en realidad existe una y sólo una función que satisface la condición propuesta. En el caso especial actual esto es bastante obvio; estamos siendo invitados a considerar el conjunto de todas aquellas parejas ordenadas $(x,$

y) de $X \times Y$ para las cuales $x = y$. Consideraciones semejantes se aplican en cada caso y, siguiendo la práctica normal de las matemáticas, usualmente describiremos una función describiendo su valor y correspondiente a cada argumento x. A veces, tal descripcion es más larga y difícil de manejar que una descripción directa del conjunto (de parejas ordenadas) involucrado, pero, no obstante, la mayor parte de los matemáticos consideran que la descripción por medio del valor del argumento es más clara que cualquier otra.

El mapeo de inclusión de X en X es conocido como la transformación *identidad* en X. (En el lenguaje de las relaciones, la identidad en X es lo mismo que la relación de igualdad en X.) Si como antes, $X \subset Y$, entonces existe una conexión entre la inclusión de X en Y y la identidad definida en Y; esta conexión es un caso especial de un proceso general empleado para formar funciones pequeñas partiendo de grandes. Si f es una función de Y a Z, digamos, y X es un subconjunto de Y, entonces existe un método natural para construir una función g de X a Z; defina a $g(x)$ como igual a $f(x)$ para cada x de X. La función g es conocida como la *restricción* de f a X, y a f se le llama *extensión* de g a Y; es usual escribir $g = f \mid X$. La definición de restricción puede expresarse escribiendo $(f \mid X)(x) = f(x)$ para cada x de X; obsérvese también que ran $(f \mid X) = f(X)$. La inclusión de un subconjunto de Y es la restricción de la identidad definida en Y, a ese subconjunto.

He aquí un ejemplo sencillo pero útil de función. Considérense dos conjuntos cualesquiera X y Y y defínase una función f de $X \times Y$ sobre X escribiendo $f(x, y) = x$. [El rigorista habrá notado que debimos escribir $f((x, y))$ en vez de $f(x, y)$, pero nunca lo hace nadie]. A la función f se le llama *proyección* de $X \times Y$ sobre X; si, análogamente, $g(x\ y) = y$, entonces g es la *proyección* de $X \times Y$ sobre Y. Aquí, la terminología está en desacuerdo con una anterior, pero no demasiado. Si $R = X \times Y$, lo que antes se llamaba proyección de R sobre la primera coordenada, es, en el presente lenguaje, el rango de la proyección f.

Un ejemplo más complicado y consecuentemente más valioso de función puede obtenerse como sigue. Supóngase que R es una relación de equivalencia en X, y sea f la función de X sobre X/R definida por $f(x) = x/R$. La función f es conocida a veces como la *transformación canónica* de X a X/R.

Si f es una función arbitraria de X sobre Y, entonces existe un método natural para definir una relación de equivalencia R en X; escríbase $a\ R\ b$ (donde a y b están en X) cuando $f(a) = f(b)$. Para cada elemento y de Y, sea $g(y)$ el conjunto de todos aquellos elementos x de X para los cuales $f(x) = y$. La definición de R implica que $g(y)$ es, para cada y, una clase de equivalencia de la relación R; en otras palabras g es una función de Y sobre el conjunto X/R de todas las clases de equivalencia de R. La función g tiene la siguiente propiedad especial: si u y v son elementos distintos de Y, entonces $g(u)$ y $g(v)$ son elementos distintos de X/R. Una función que transforma elementos distintos en elementos distintos es llamada *uno a uno* (usualmente una correspondencia *uno a uno*). Entre los ejemplos anteriores, las transformaciones de inclusión son *uno a uno*, pero, excepto en algunos casos especiales triviales, las proyecciones no lo son. (Ejercicio: ¿qué casos especiales?)*

Para introducir el siguiente aspecto de la teoría elemental de las funciones haremos una disgresión y anticiparemos un pequeño fragmento de nuestra definición fundamental de números naturales. No necesitaremos definir ahora todos los números naturales; todo lo que necesitamos son los tres primeros. Ya que no es ésta la ocasión apropiada para preliminares heurísticos prolongados, procederemos directamente con la definición pese al riesgo de molestar o preocupar temporalmente a algunos lectores. Hela aquí: definimos 0, 1 y 2 en la forma

$$0 = \varnothing,\ 1 = \{\varnothing\}\ \text{y}\ 2 = \{\varnothing,\ \{\varnothing\}\}.$$

En otras palabras, 0 es vacío, 1 es el conjunto singular $\{0\}$ y 2 es la pareja $\{0, 1\}$. Obsérvese que hay cierto método en esta aparente demencia; el número de elementos en los conjuntos 0, 1 o 2 (en el sentido ordinario usual de la palabra) es, respectivamente, cero, uno o dos.

Si A es un subconjunto de un conjunto X, la *función característica* de A es la función χ de X a 2 tal que $\chi(x) = 1$ o

*Una función que a elementos distintos asocia elementos distintos es una *función de tipo uno a uno* siguiendo a la terminología inglesa y *función biunívoca* siguiendo a la terminología francesa. Ambas terminologías tienen aproximadamente la misma aceptación. Una función uno a uno de A en B *no toma necesariamente todos los valores de* B a menos que sea *sobre* B; en el presente libro, sin embargo, se entiende que una correspondencia uno a uno *entre* A y B toma efectivamente todos los valores de B. Otros términos usados son: *función inyectiva* (uno a uno) *suprayectiva* (*sobre*) y *biyectiva* (uno a uno y sobre). N. del R.

0, según que $x \in A$ o $x \in X - A$. El hecho de que la función característica de A depende del conjunto A puede indicarse escribiendo χ_A en vez de χ. La función que asigna a cada subconjunto A de X [esto es, a cada elemento de $\mathcal{P}(X)$] la función característica de A (esto es, un elemento de 2^X) es una correspondencia uno a uno entre $\mathcal{P}(X)$ y 2^X. (Entre paréntesis; en lugar de la frase "la función que asigna a cada A de $\mathcal{P}(X)$" el elemento χ_A en 2^X se acostumbra emplear la abreviatura "la función $A \to \chi_A$". En este lenguaje, la proyección de $X \times Y$ sobre X, por ejemplo, será descrita como la función $(x, y) \to x$, y la transformación canónica de un conjunto X con una relación R sobre X/R será descrita como la función $x \to x/R$).

EJERCICIO. (i) $Y^{\varnothing}$ tiene exactamente un elemento, a saber, $\varnothing$ independientemente de que Y sea o no vacío, y (ii) si X no es vacío, entonces $\varnothing^X$ es vacío.

SECCION 9

FAMILIAS

Hay ocasiones en que el rango de una función es considerado como más importante que la función misma. Cuando éste es el caso, tanto la terminología como la notación sufren alteraciones radicales. Supóngase, por ejemplo, que x es una función de un conjunto I a un conjunto X. (La sola elección de las letras indica que algo extraño se está preparando.) Un elemento del dominio I es conocido como un *índice*, a I se le llama *conjunto de índices*, el rango de la función es denominado *conjunto indicado*,* la función misma recibe el nombre de *familia* y el valor de la función x correspondiente a un índice i, se denota por x_i, y es llamado *término* de la familia. (Esta terminología no es absoluta y es una de entre varias que difieren ligeramente; será la única que usemos en lo sucesivo.) Una manera inaceptable, pero generalmente aceptada de comunicar la notación e indicar el énfasis, es hablar de una familia $\{x_i\}$ en X o de una familia $\{x_i\}$ de elementos de X cualesquiera que éstos puedan ser; cuando es necesario, el conjunto I de índices se indica mediante expresiones entre paréntesis tales como $(i \in I)$. Así, por ejemplo, se interpreta usualmente que la frase "una familia $\{A_i\}$ de subconjuntos de X" se refiere a una función A, de un conjunto I de índices en $\mathcal{P}(X)$.

Si $\{A_i\}$ es una familia de subconjuntos de X, la unión del rango de la familia es llamado unión de la familia $\{A_i\}$, o unión de los conjuntos A_i; la notación acostumbrada para de-

* En lo sucesivo téngase cuidado en determinar si lo *indicado* está *indicado* en este sentido matemático. (N. del R.)

signarla es

$$\bigcup_{i \epsilon I} A_i \quad \text{o} \quad \bigcup_i A_i,$$

según si es o no importante hacer resaltar al conjunto de índices I. De la definición de uniones se sigue inmediatamente que $x \epsilon \bigcup_i A_i$ si y sólo si x pertenece a A_i cuando menos para una i. Si $I = 2$, de manera que el rango de la familia $\{A_i\}$ es la pareja no ordenada $\{A_0, A_1\}$, entonces $\bigcup_i A_i = A_0 \cup A_1$. Obsérvese que no se pierde generalidad al considerar familias de conjuntos en lugar de colecciones arbitrarias de conjuntos, ya que toda colección de conjuntos es el rango de alguna familia. Si $\mathcal{C}$ es una colección de conjuntos, permítase que $\mathcal{C}$ misma haga las veces del conjunto de índices, y tómese la transformación identidad sobre $\mathcal{C}$ para el papel de la familia.

Las leyes algebraicas satisfechas por la operación de unión de parejas pueden ser generalizadas a uniones arbitrarias. Supóngase, por ejemplo, que $\{I_j\}$ es una familia de conjuntos cuyo dominio es, digamos, J; escríbase $K = \bigcup_j I_j$, y sea $\{A_k\}$ una familia de conjuntos con dominio K. No es difícil entonces demostrar que

$$\bigcup_{k \epsilon K} A_k = \bigcup_{j \epsilon J} (\bigcup_{i \epsilon I_j} A_i);$$

ésta es la versión generalizada de la ley asociativa para uniones. Ejercicio: formule y demuestre una versión generalizada de la ley conmutativa.

Tiene sentido hablar de una unión vacía (y es vacía), pero no tiene sentido hablar de una intersección vacía. Con excepción de lo referente a esta trivialidad, la terminología y notación empleada para las intersecciones semeja punto por punto a la de las uniones. Así por ejemplo, si $\{A_i\}$ es una familia no vacía de conjuntos, la intersección del rango de la familia es llamada intersección de la familia $\{A_i\}$, o intersección de los conjuntos A_i; la notación acostumbrada para designarla es

$$\bigcap_{i \epsilon I} A_i \quad \text{o} \quad \bigcap_i A_i,$$

según si es o no importante hacer resaltar al conjunto de índices I. (Por "familia no vacía" entendemos una familia cuyo dominio I no es vacío). De la definición de intersecciones se sigue de inmediato que si $I \neq \varnothing$, entonces una condición ne-

cesaria y suficiente para que x pertenezca a $\bigcap_i A_i$ es que x pertenezca a A_i para todo i.

Las leyes conmutativa y asociativa generalizadas pueden formularse y demostrarse para intersecciones en la misma forma que para uniones, o, alternativamente, pueden ser empleadas las leyes De Morgan para derivarlas a partir de las propiedades de las uniones. Esto es casi obvio, y, por lo tanto, no tiene mucho interés. Las identidades algebraicas interesantes son aquellas que involucran tanto a uniones como a intersecciones Así. por ejemplo, si $\{A_i\}$ es una familia de subconjuntos de X y $B \subset X$, entonces

$$B \cap \bigcup_i A_i = \bigcup_i (B \cap A_i)$$

y

$$B \cup \bigcap_i A_i = \bigcap_i (B \cup A_i);$$

estas ecuaciones son una ligera generalización de las leyes distributivas.

EJERCICIO. Si tanto $\{A_i\}$ como $\{B_j\}$ son familias de conjuntos, entonces

$$(\bigcup_i A_i) \cap (\bigcup_j B_j) = \bigcup_{i,j} (A_i \cap B_j)$$

y

$$(\bigcap_i A_i) \cup (\bigcap_j B_j) = \bigcap_{i,j} (A_i \cup B_j).$$

Explicación de la notación: un símbolo tal como $\bigcup_{i,j}$ es una abreviación de $\bigcup_{(i,j)\in I \times J}$.

La notación de familias es la que se emplea normalmente para generalizar el concepto de producto cartesiano. El producto cartesiano de dos conjuntos X y Y fue definido como el conjunto de las parejas ordenadas (x, y) con x en X y y en Y. Existe una correspondencia uno a uno entre este conjunto y cierto conjunto de familias. En efecto, considérese una pareja no ordenada cualquiera $\{a, b\}$ con $a \neq b$, y considérese el conjunto Z de todas las familias z, indicadas por $\{a, b\}$ tales que $z_a \in X$ y $z_b \in Y$. Si la función f de Z a $X \times Y$ es definida como $f(z) = (z_a, z_b)$, entonces f es la correspondencia uno a uno mencionada. La diferencia entre Z y $X \times Y$ es tan sólo cuestión de notación. La generalización de productos cartesianos generaliza más bien a Z que al mismo $X \times Y$. (Resulta como consecuencia una ligera desavenencia en la terminología al pasar del caso especial al general. No

hay manera de evitarla; así es como el lenguaje matemático se usa actualmente.) La generalización está ahora libre de contratiempos. Si $\{X_i\}$ es una familia de conjuntos ($i \in I$), el *producto cartesiano* de la familia es, por definición, el conjunto de todas las familias $\{x_i\}$ con $x_i \in X_i$ para cada i de I. Existen en uso más o menos corriente varios símbolos para el producto cartesiano; en este libro lo denotaremos por

$$\times_{i \in I} X_i \quad \text{o} \quad \times_i X_i.$$

Es claro que si todo X_i es igual a un mismo conjunto X, entonces $\times_i X_i = X^I$. Si I es una pareja $\{a, b\}$ con $a \neq b$, entonces se acostumbra identificar a $\times_{i \in I} X_i$ con el producto cartesiano $X_a \times X_b$ como fue definido primero, y si I es un conjunto singular $\{a\}$, entonces, análogamente, identificamos a $\times_{i \in I} X_i$ con X_a mismo. *Ternas ordenadas, cuaternas ordenadas,* etc., pueden ser definidas como familias cuyos conjuntos de índices son ternas, cuaternas, etc., no ordenadas.

Supóngase que $\{X_i\}$ es una familia de conjuntos ($i \in I$) y sea X su producto cartesiano. Si J es un subconjunto de I, entonces a cada elemento de X corresponde de una manera natural un elemento del producto cartesiano parcial $\times_{i \in J} X_i$. Para definir la correspondencia, recuérdese que cada elemento x de X es en sí mismo una familia $\{x_i\}$, o sea, según el último análisis, una función en I; el elemento correspondiente, digamos y, de $\times_{i \in J} X_i$ se obtiene por una simple restricción de esa función a J. Explícitamente, escribiremos $y_i = x_i$ siempre que $i \in J$. La correspondencia $x \to y$ es conocida como la proyección de X sobre $\times_{i \in J} X_i$ y la denotaremos temporalmente por f_J. Si, en particular J es un conjunto singular, digamos $J = \{j\}$, entonces escribiremos f_j (en lugar de $f_{\{j\}}$) por f_J. La palabra "proyección" tiene múltiples usos; si $x \in X$, el valor de f_j tomado en x, o sea x_j, también es conocido como la proyección de x sobre X_j o, alternativamente, la j-ésima coordenada de x. Una función en un producto cartesiano tal como X es llamada función de *varias variables* y, en particular, una función en el producto cartesiano $X_a \times X_b$ es conocida como una función de dos variables.

Ejercicio. Demuestre que $(\bigcup_i A_i) \times (\bigcup_j B_j) = \bigcup_{i,j} (A_i \times B_j)$ y que la misma ecuación se cumple para inter-

secciones (siempre que los dominios de las familias consideradas no sean vacíos). Demuestre también (con estipulaciones apropiadas acerca de las familias vacías) que $\bigcap_i X_i \subset X_j \subset \bigcup_i X_i$ para cada índice j y que esta intersección y esta unión pueden, de hecho, ser caracterizadas como las soluciones extremas de estas inclusiones. Esto significa que si $X_j \subset Y$ para cada índice j, entonces $\bigcup_i X_i \subset Y$ y que $\bigcup_i X_i$ es el único conjunto que satisface esta inclusión con respecto a cualquier Y de las especificadas; la formulación para intersecciones es semejante.

SECCION 10

FUNCIONES INVERSAS Y COMPUESTAS

Asociada con cada función f de X a Y, digamos, hay una función de $\mathcal{P}(X)$ a $\mathcal{P}(Y)$, a saber, la función (frecuentemente denotada también por f) que asocia a cada subconjunto A de X el subconjunto imagen $f(A)$ de Y. El comportamiento algebraico del mapeo $A \rightarrow f(A)$ deja algo que desear. Es cierto que si $\{A_i\}$ es una familia de subconjuntos de X, entonces $f(\bigcup_i A_i) = \bigcup_i f(A_i)$ (¿demostración?), pero la ecuación correspondiente para intersecciones es generalmente falsa (¿ejemplo?), y la conexión entre imágenes y complementos es igualmente insatisfactoria.

Una correspondencia entre los elementos de X y los elementos de Y induce siempre una correspondencia de buen comportamiento entre los subconjuntos de X y los subconjuntos de Y, no hacia adelante, mediante la formación de imágenes, sino hacia atrás mediante la formación de imágenes inversas. Dada una función f de X a Y, sea f^{-1}, *inversa* de f, la función de $\mathcal{P}(Y)$ a $\mathcal{P}(X)$ tal que si $B \subset Y$ se tenga

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

En palabras: $f^{-1}(B)$ está constituido precisamente por aquellos elementos de X que f transforma en elementos de B; el conjunto $f^{-1}(B)$ es llamado *imagen inversa* de B bajo f. Una condición necesaria y suficiente para que f transforme a X *sobre* Y es que la imagen inversa bajo f de cada subconjunto no vacío de Y sea un subconjunto no vacío de X. (¿Demostración?) Una condición necesaria y suficiente para que f sea uno a uno es que la imagen inversa bajo f de cada conjunto singular* del rango de f sea un conjunto singular en X.

* Definición de conjunto singular en la Pág. 19.

Si la última condición se satisface, entonces al símbolo f^{-1} se le interpreta frecuentemente de una segunda manera, a saber, como la función cuyo dominio es el rango de f y cuyo valor para cada y del rango de f es el único x de X para el cual $f(x) = y$. En otras palabras, para funciones f uno a uno, podemos escribir $f^{-1}(y) = x$ si y sólo si $f(x) = y$. Este empleo de la notación es ligeramente inconsistente con nuestra primera interpretación de f^{-1}, pero no es probable que el doble significado conduzca a una confusión.

La conexión entre imágenes e imágenes inversas merece una deliberación momentánea.

Si $B \subset Y$, entonces

$$f(f^{-1}(B)) \subset B.$$

Demostración. Si $y \in f[f^{-1}(B)]$, entonces $y = f(x)$ para algún x de $f^{-1}(B)$, lo cual significa que $y = f(x)$ y $f(x) \in B$. y por lo tanto $y \in B$.

Si f transforma a X *sobre* Y, entonces

$$f(f^{-1}(B)) = B.$$

Demostración. Si $y \in B$, entonces $y = f(x)$ para algún x de X y, consecuentemente, para alguna x de $f^{-1}(B)$; esto significa que $y \in f[f^{-1}(B)]$.

Si $A \subset X$, entonces

$$A \subset f^{-1}(f(A)).$$

Demostración. Si $x \in A$, entonces $f(x) \in f(A)$, lo cual significa que $x \in f^{-1}[f(A)]$.

Si f es uno a uno, entonces

$$A = f^{-1}(f(A)).$$

Demostración. Si $x \in f^{-1}[f(A)]$, entonces $f(x) \in f(A)$ de manera que $f(x) = f(u)$ para algún u de A; esto implica que $x = u$, y, por lo tanto, que $x \in A$.

El comportamiento algebraico de f^{-1} es intachable. Si $\{B_i\}$ es una familia de subconjuntos de Y, entonces

$$f^{-1}(\bigcup_i B_i) = \bigcup_i f^{-1}(B_i)$$

y

$$f^{-1}(\bigcap_i B_i) = \bigcap_i f^{-1}(B_i).$$

Las demostraciones son directas. Si, por ejemplo, $x \in f^{-1}(\bigcap_i B_i)$, entonces $f(x) \in B_i$ para todo i, de manera que $x \in$

$f^{-1}(B)$ para todo i, y por lo tanto, $x \in \bigcap_i f^{-1}(B_i)$; todos los pasos de este proceso son reversibles. La formación de imágenes inversas también conmuta con la complementación; esto es,

$$f^{-1}(Y - B) = X - f^{-1}(B)$$

para cada subconjunto B de Y. De hecho: si $x \in f^{-1}(Y - B)$, entonces $f(x) \in Y - B$ de manera que $x \in' f^{-1}(B)$ y, por lo tanto $x \in X - f^{-1}(B)$; los pasos son reversibles. (Obsérvese que la última ecuación es, en realidad, una forma de ley conmutativa; establece que la complementación seguida de la inversión es lo que la inversión seguida de la complementación.)

El estudio de las inversas deja ver que lo que hace una función puede en cierto sentido, ser deshecho; lo que veremos en seguida es que lo que las funciones hacen puede a veces ser hecho en un paso. Para ser explícitos, si f es una función de X a Y y g es una función de Y a Z, entonces todo elemento del rango de f pertenece al dominio de g, y, consecuentemente, $g[f(x)]$ tiene sentido para cada x de X. La función h de X a Z, definida por $h(x) = g\,[f(x)]$ es conocida como la *composición* de las funciones f y g, y es denotada por $g \circ f$ o, más simplemente, por gf. (Ya que no tendremos ocasión de considerar ninguna otra clase de multiplicación de funciones, en este libro usaremos solamente la última notación, que es la más simple.)

Obsérvese que el orden de los sucesos es importante en la teoría de la composición funcional. Con el fin de que gf esté definida, el rango de f debe estar incluido en el dominio de g y esto puede suceder sin que necesariamente esté sucediendo en el otro sentido al mismo tiempo. Aún si ambas fg y gf están definidas, lo cual sucede si, por ejemplo, f transforma a X en Y y g transforma a Y en X, las funciones fg y gf no tienen que ser iguales, en otras palabras, la composición funcional no tiene que ser conmutativa.

La composición funcional puede no ser conmutativa, pero es siempre asociativa. Si f transforma a X en Y, g a Y en Z y h a Z en U, podemos formar entonces la composición de h con gf y la composición de hg con f; es un ejercicio simple hacer ver que el resultado es el mismo en cualquier caso.

La conexión entre la inversión y la composición es importante; algo por el estilo se deja ver a lo largo de todas las matemáticas. Si f transforma a X en Y y g transforma a Y en Z, en-

tonces f^{-1} transforma a $\mathcal{P}(Y)$ en $\mathcal{P}(X)$ y g^{-1} transforma a $\mathcal{P}(Z)$ en $\mathcal{P}(Y)$. En esta situación, las composiciones que pueden formarse son gf y $f^{-1}g^{-1}$ y lo que se afirma es que la última es la inversa de la primera. Demostración: si $x \in (gf)^{-1}(C)$, donde $x \in X$ y $C \subset Z$, entonces $g[f(x)] \in C$, de manera que $f(x) \in g^{-1}(C)$, y, por lo tanto, $x \in f^{-1}[g^{-1}(C)]$; los pasos del argumento son reversibles.

La inversión y la composición de funciones son casos especiales de operaciones semejantes definidas para las relaciones. Así en particular, asociada con cada relación R de X a Y está la relación *inversa* R^{-1} de Y a X; por definición, $y\, R^{-1} x$ significa que $x\, R\, y$. Ejemplo: Si R es la relación de pertenencia, de X a $\mathcal{P}(X)$, entonces R^{-1} es la relación de continencia* de $\mathcal{P}(X)$ a X. Una consecuencia inmediata de las definiciones consideradas es que dom R^{-1} = ran R y ran R^{-1} = dom R. Si la relación R es una función, entonces las aseveraciones equivalentes $x\, R\, y$ y $y\, R^{-1}\, x$ pueden ser escritas en las formas equivalentes $R(x) = y$ y $x \in R^{-1}(\{y\})$.

A causa de dificultades con la conmutatividad, la generalización de la composición funcional debe manejarse con cuidado. La composición de las relaciones R y S está definida en el caso en que R es una relación de X a Y, y S una relación de Y a Z. La relación compuesta T de X a Z se denota por $S \circ R$ o, simplemente, por SR, y está definida de manera que $x\, T\, z$ si y sólo si existe un elemento y en Y tal que $x\, R\, y$ y $y\, S\, z$. Como un ejemplo instructivo, permítase que R signifique "hijo" y S signifique "hermano" en el conjunto de los varones. En otras palabras, $x\, R\, y$ significa que x es un hijo de y, y $y\, S\, z$ que y es un hermano de z. En este caso la relación compuesta SR significa "sobrino". (Pregunta: ¿qué significan R^{-1}, S^{-1}, RS y $R^{-1}S^{-1}$,?) Si tanto R como S son funciones, entonces $x\, R\, y$ y $y\, S\, z$ pueden reescribirse en la forma $R(x) = y$ y $S(y) = z$, respectivamente. Se sigue que $S[R(x)] = z$ si y sólo si $x\, T\, z$, de modo que la composición funcional es de hecho un caso especial de lo que a veces es llamado *producto relativo*.

Las propiedades algebraicas de la inversión y de la composición son las mismas para las relaciones y para las funciones Así, en particular, la composición es conmutativa sólo por

* Acción de contener según el Dicc. de la Lengua.

accidente, pero es siempre asociativa, y en todos los casos está conectada con la inversión por medio de la ecuación $(SR)^{-1} = R^{-1}S^{-1}$. (¿Demostraciones?)

El álgebra de las relaciones produce algunas fórmulas divertidas. Supóngase que, temporalmente, consideramos relaciones sólo en un conjunto X, y, en particular, permítase que sea I la relación de igualdad en X (lo cual es lo mismo que la transformación identidad de X sobre X). La relación I actúa como una unidad multiplicativa, lo cual significa que $IR = RI = R$ para toda relación R en X. Pregunta: ¿existe una conexión entre I, RR^{-1} y $R^{-1}R$? Las tres propiedades que definen una relación de equivalencia pueden ser expresadas en términos algebraicos en la forma siguiente: la reflexividad significa que $I \subset R$, la simetría significa que $R \subset R^{-1}$ y la transitividad significa que $RR \subset R$.

EJERCICIO. (Supóngase en cada caso que f es una función de X a Y.) (*i*) Si g es una función de Y a X tal que gf es la identidad en X entonces f es uno a uno y g transforma a Y sobre X. (ii) Una condición necesaria y suficiente para que $f(A \cap B) = f(A) \cap f(B)$ para todos los subconjuntos A y B de X es que f sea uno a uno. (iii) Una condición necesaria y suficiente para que $f(X - A) \subset Y - f(A)$ para todos los subconjuntos A de X es que f sea uno a uno. (iv) Una condición necesaria y suficiente para que $Y - f(A) \subset f(X - A)$ para todos los subconjuntos A de X es que f transforme a X sobre Y.

SECCION 11

NUMEROS

¿Qué tanto es dos? Más generalmente, ¿cómo vamos a definir los números? Para prepararnos a la respuesta, consideremos un conjunto X y formemos la colección P de todas las parejas no ordenadas $\{a, b\}$ con a en X, b en X y $a \neq b$. Parece ser claro que todos los conjuntos de la colección P tienen una propiedad común, la propiedad de estar constituidos por dos elementos. Es tentador el tratar de definir el concepto "dos" como la propiedad común de todos los conjuntos de la colección P, pero la tentación debe ser resistida; después de todo tal definición es matemáticamente sin sentido. ¿Qué es una propiedad? ¿Cómo sabemos que todos los conjuntos de P tienen sólo una propiedad común?

Tal vez después de meditar un poco podamos encontrar una manera de preservar la idea que hay detrás de la definición propuesta sin tener que usar expresiones vagas tales como "la propiedad común". Una práctica matemática ubicua es la de identificar a una propiedad con un conjunto, a saber, con el conjunto de todos los objetos que poseen la propiedad; ¿por qué no hacerlo aquí? En otras palabras, ¿por qué no definir "dos" como el conjunto P? Algo por el estilo se hace a veces, pero no es del todo satisfactorio. El problema es que nuestra proposición modificada actual depende de P, y por lo tanto, en última instancia, de X. Cuando mucho, la proposición define al concepto "dos" para subconjuntos de X; no sugiere ninguna idea de cuándo vamos a atribuir dicho concepto a un subconjunto que no esté incluido en X.

Hay dos caminos por seguir. Uno consiste en abandonar la restricción a un conjunto particular y considerar en vez de esto a todas las parejas no ordenadas $\{a, b\}$ con $a \neq b$. Estas

parejas no ordenadas no constituyen un conjunto; para poder basar en ellas la definición de "dos" es necesario extender toda la teoría bajo consideración a modo de que incluya los "no-conjuntos" (clases) de otra teoría. Esto puede hacerse, pero no será hecho aquí; seguiremos un camino distinto.

¿Cómo sería definido un metro por un matemático? El procedimiento análogo al bosquejado anteriormente comprendería los dos pasos siguientes. Primero, escójase un objeto que sea uno de los modelos deseados del concepto a ser definido—en otras palabras, un objeto tal que en el aspecto intuitivo o práctico merezca ser llamado un metro de longitud, si es que algo lo merece. Segundo, fórmese el conjunto de todos los objetos del universo que tengan la misma longitud que el elegido (nótese que esto no depende del conocimiento de lo que es un metro), y defina como un metro al conjunto así formado.

¿Cómo se define en realidad un metro? el ejemplo fue elegido de manera que la contestación a esta pregunta sugiera una vía de entrada a la definición de los números. El punto es que en la definición acostumbrada de un metro se omite el segundo paso. Por razón de un acuerdo más o menos arbitrario, se elige un objeto y se llama metro a su longitud. Si la definición acusa circularidad (¿qué significa "longitud"?), puede ser fácilmente convertida en una definición demostrativa irrecusable; después de todo, no hay nada que nos impida definir al metro como aquello igual al objeto elegido. Si se adopta este punto de vista demostrativo, es tan fácil como antes explicar cuándo se debe atribuir la propiedad "un-metro" a algún otro objeto, a saber, sólo en el caso de que el nuevo objeto tenga la misma longitud que el patrón elegido. Anotamos otra vez que la determinación de cuándo dos objetos tienen o no la misma longitud, depende solamente de un simple acto de comparación y no de que se tenga una definición precisa de longitud.

Motivados por las consideraciones descritas anteriormente, habíamos definido al 2 como cierto conjunto particular con dos elementos exactamente* (hablando en forma intuitiva). ¿Cómo se eligió este conjunto patrón? ¿Cómo deberán ser elegidos otros de estos conjuntos patrón para otros números? No hay ninguna razón matemática apremiante para preferir una respuesta a esta pregunta y no otra; todo el asunto es en gran ma-

* Véase Pág. 50. N. del R.

nera cuestión de gustos. Presumiblemente, la selección debe ser orientada por consideraciones de simplicidad y economía. Para motivar la selección particular que usualmente se hace, supóngase que un número, digamos 7, ha sido definido ya como un conjunto (con siete elementos). En este caso, cómo definiremos al 8? En otras palabras, ¿dónde vamos a encontrar un conjunto constituido precisamente por ocho elementos? Podemos encontrar siete elementos en el conjunto 7; ¿qué tomaremos como un octavo elemento que agregarles? Una respuesta razonable para la última pregunta es el número (conjunto) 7 mismo; lo que se propone es definir al 8 como el conjunto constituido por los siete elementos de 7, y 7. Obsérvese que de acuerdo con esta proposición cada número será igual al conjunto formado por los que le preceden.

El párrafo anterior motiva una construcción en la teoría de los conjuntos que tiene sentido para todo conjunto, pero que sólo interesa para la construcción de números. Para cada conjunto x definimos al sucesor x^+ de x como el conjunto obtenido al agregar x a los elementos de x; en otras palabras,

$$x^+ = x \cup \{x\}.$$

(El sucesor de x es denotado frecuentemente por x').

Ahora estamos listos para definir a los números naturales. Para definir al 0 como un conjunto con cero elementos no tenemos alternativa; debemos escribir, (como lo hicimos)

$$0 = \varnothing.$$

Si cada número natural ha de ser igual al conjunto de sus predecesores, tampoco tenemos alternativa al definir al 1, al 2, al 3; debemos escribir

$$1 = 0^+ \ (= \{0\}),$$
$$2 = 1^+ \ (= \{0, 1\}),$$
$$3 = 2^+ \ (= \{0, 1, 2\}),$$

etc. El "etc." significa que de aquí en adelante adoptamos la notación usual y, en lo que sigue, nos sentiremos libres de usar numerales tales como "4" o "956" sin ninguna explicación adicional o apología.

De lo que se ha dicho hasta el momento no se sigue que la construcción de sucesores puede ser llevada al infinito dentro de un mismo conjunto. Lo que necesitamos es un nuevo principio en la teoría de los conjuntos.

Axioma del infinito. *Existe un conjunto que contiene al 0 y al sucesor de cada uno de sus elementos.*

La causa del nombre del axioma debe estar clara. No hemos dado aún una definición precisa de infinito, pero parece razonable que conjuntos tales como los que describe el axioma del infinito merecen ser llamados infinitos.

Diremos temporalmente que un conjunto A es un *conjunto de sucesores* si $0 \in A$ y si $x^+ \in A$ siempre que $x \in A$. Con este lenguaje el axioma del infinito dice simplemente que existe un conjunto de sucesores A. Como la intersección de cada familia (no vacía) de conjuntos de sucesores es a su vez un conjunto de sucesores (¿demostración?), la intersección de todos los conjuntos de sucesores incluidos en A es un conjunto de sucesores ω. El conjunto ω es un subconjunto de cada conjunto de sucesores. En efecto, si B es un conjunto de sucesores arbitrario, entonces también lo es $A \cap B$. Ya que $A \cap B \subset A$, el conjunto $A \cap B$ es uno de los conjuntos que intervienen en la definición de ω, y se sigue que $\omega \subset A \cap B$, y, consecuentemente, que $\omega \subset B$. La propiedad de "minimalidad" así establecida caracteriza al conjunto ω en forma única; el axioma de la extensión garantiza que sólo puede haber un conjunto de sucesores que esté incluido en cualquier otro conjunto de sucesores. Un *número natural*, es por definición, un elemento del conjunto de sucesores mínimo ω. Esta definición de los números naturales es la contraparte rigurosa de la descripción intuitiva, de acuerdo con la cual consisten en 0, 1, 2, 3, "y así sucesivamente". A propósito, el símbolo que estamos empleando para denotar al conjunto de todos los números naturales (ω) tiene aceptación de parte de quienes escriben sobre la materia, pero en ninguna forma de parte de una mayoría clara. En el presente libro se usará ese símbolo sistemática y exclusivamente en el sentido definido con anterioridad.

La ligera sensación de incomodidad que posiblemente experimente el lector en relación con la definición de los números naturales es bastante común, y, en la mayoría de casos, temporal.

El problema es que aquí, como sucedió una vez antes (en la definición de parejas ordenadas), el objeto definido tiene ciertas estructuras que no vienen al caso y que parecen atravesarse en el camino (pero esto, de hecho, es inofensivo). Deseamos oír que el sucesor de 7 es 8, pero que se nos diga que 7 es un subconjunto de 8 o que 7 es un elemento de 8, nos perturba. Haremos uso de esta superestructura de los números naturales sólo lo necesario para deducir sus propiedades naturales más importantes; después de esto la superestructura puede ser olvidada sin peligro alguno.

Una familia $\{x_i\}$ cuyo conjunto de índices es un número natural, o bien, es el conjunto de todos los números naturales, se conoce como una *sucesión* (*finita* o *infinita*, respectivamente). Si $\{A_i\}$ es una sucesión de conjuntos, donde el conjunto de índices es el número natural n^+, entonces la unión de la sucesión es denotada por

o $$\bigcup_{i=0}^{n} A_i \quad \text{o} \quad A_0 \cup \cdots \cup A_n.$$

Si el conjunto de índices es ω, la notación es

$$\bigcup_{i=0}^{\infty} A_i \quad \text{o} \quad A_0 \cup A_1 \cup A_2 \cup \cdots.$$

Las intersecciones y los productos cartesianos de sucesiones son denotados análogamente por

$$\bigcap_{i=0}^{n} A_i, \quad A_0 \cap \cdots \cap A_n,$$
y $$\times_{i=0}^{n} A_i, \quad A_0 \times \cdots \times A_n,$$

$$\bigcap_{i=0}^{\infty} A_i, \quad A_0 \cap A_1 \cap A_2 \cap \cdots,$$
$$\times_{i=0}^{\infty} A_i, \quad A_0 \times A_1 \times A_2 \times \cdots.$$

la palabra "sucesión" es usada en la literatura matemática de unas cuantas maneras diferentes, pero las diferencias entre ellas son más de notación que de concepto. La alternativa más común comienza con 1 en lugar de 0; en otras palabras, se refiere a una familia cuyo conjunto de índices es $\omega - \{0\}$ en vez de ω.

SECCION 12

LOS AXIOMAS DE PEANO

Ahora iniciaremos una digresión menor. El propósito de la misma es el de hacer un contacto efímero con la teoría aritmética de los números naturales. Desde el punto de vista de la teoría de los conjuntos esto es un lujo agradable.

El hecho más importante que conocemos acerca del conjunto ω de todos los números naturales es el siguiente: ω es el único conjunto de sucesores que es subconjunto de cualquier conjunto de sucesores. Decir que ω es un conjunto de sucesores significa que

(I)
$$0 \in \omega$$

(donde, por supuesto, $0 = \varnothing$), y que

(II) *si* $n \in \omega$, *entonces* $n^{+} \in \omega$

(donde $n^{+} = n \cup \{n\}$). La propiedad de "minimalidad" de ω puede ser expresada diciendo que si un subconjunto S de ω es un conjunto de sucesores, entonces $S = \omega$. De otra manera, en términos más primitivos.

(III) si

$S \subset \omega$, *si* $0 \in S$ *y si* $n^{+} \in S$ *siempre que* $n \in S$, *entonces* $S = \omega$.

La propiedad (III) es conocida como el **principio de inducción matemática.** Agregaremos ahora a la lista de propiedades de ω otras dos:

(IV) $n^{+} \neq 0$ *para todo* n *en* ω,

y

(V) *si* n *y* m *están en* ω, *y si* $n^{+} = m^{+}$, *entonces* $n = m$.

La demostración de (IV) es trivial; como n^+ siempre contiene a n, y ya que 0 es vacío, es claro que n^+ es distinto de 0. La demostración de (V) no es trivial; depende de un par de proposiciones auxiliares. La primera de ellas afirma que algo que no debe suceder, en realidad no sucede. Aún si las consideraciones involucradas en la demostración parecen ser patológicas y ajenas al espíritu aritmético que esperamos encontrar en la teoría de los números naturales, el fin justifica los medios. La segunda se refiere a un proceder bastante parecido al que se acaba de rechazar. Sin embargo, en esta ocasión las consideraciones aparentemente artificiales desembocan en un resultado afirmativo: siempre sucede algo ligeramente sorpresivo. Las proposiciones son las siguientes: (i) *ningún número natural es un subconjunto de alguno de sus elementos*, y (ii) *todo elemento de un número natural es un subconjunto de éste*. Algunas veces un conjunto con la propiedad de que incluye ($\subset$) a todo lo que contiene (ϵ) es llamado conjunto *transitivo*. Más precisamente, decir que E es transitivo significa que si $x \epsilon y$ y $y \epsilon E$, entonces $x \epsilon E$. (Recuérdese el uso ligeramente distinto de la palabra, dado en la teoría de las relaciones.) Con este lenguaje, (ii) dice que todo número natural es transitivo.

La demostración de (i) es una aplicación típica del principio de inducción matemática. Sea S el conjunto de todos aquellos números naturales n que no están incluidos en ninguno de sus elementos. (Explícitamente: $n \epsilon S$ si y sólo si $n \epsilon \omega$ y n no es subconjunto de ninguno de sus elementos). Como 0 no es un subconjunto de alguno de sus elementos, se sigue que $0 \epsilon S$. Supóngase ahora que $n \epsilon S$. Como n es un subconjunto de n, podemos inferir que n no es un elemento de n, y por lo tanto, que n^+ no es un subconjunto de n. ¿De qué puede ser n^+ un subconjunto? si $n^+ \subset x$, entonces $n \subset x$, y, por lo tanto, (como $n \epsilon S$) $x \epsilon' n$. Se sigue que n^+ no puede ser un subconjunto de n. y que n^+ no puede ser un subconjunto de ningún elemento de n. Esto significa que n^+ no puede ser un subconjunto de ningún elemento de n^+, y, por lo tanto, que $n^+ \epsilon S$. La conclusión deseada (i) es entonces una consecuencia de (III).

La demostración de (ii) es también por indución. Sea ahora S el conjunto de todos los números naturales transitivos. (Explícitamente: $n \epsilon S$ si y sólo si $n \epsilon \omega$ y x es un subconjunto de n para todo x de n). El requerimiento de que $0 \epsilon S$ es sa-

tisfecho por vacuidad. Supóngase ahora que $n \in S$. Si $x \in n^+$, entonces o $x \in n$ o $x = n$. En el primer caso $x \subset n$ (ya que $n \in S$) y por consiguiente $x \subset n^+$; en el segundo caso $x \subset n^+$ por razones aún más triviales. Se sigue que todo elemento de n^+ es un subconjunto de n^+, o, en otras palabras, que $n^+ \in S$. La conclusión deseada (ii) es entonces una consecuencia de (III).

Ahora estamos listos para demostrar (V). Supóngase que en realidad n y m son números naturales y que $n^+ = m^+$. Como $n \in n^+$, se sigue que $n \in m^+$ y, por lo tanto, que $n \in m$ o que $n = m$. Análogamente, o $m \in n$ o $m = n$. Si $n \neq m$, entonces debemos tener $n \in m$ y $m \in n$. Como, por (ii), n es transitivo, se sigue que $n \in n$. Sin embargo, como $n \subset n$, esto contradice a (i), lo cual completa la demostración.

Las proposiciones (I)–(V) son conocidas como los axiomas de Peano, y usualmente se les considera como la fuente del conocimiento matemático. A partir de ellos (junto con los principios de la teoría de los conjuntos que hemos presentado) es posible definir a los enteros, a los números racionales, a los números reales y a los números complejos, así como deducir sus propiedades aritméticas y analíticas. Tal programa no está dentro del campo de este libro; el lector interesado no tendrá dificultad para encontrarlo y estudiarlo en otra parte.

La inducción se usa con frecuencia no solamente para demostrar cosas, sino también para definirlas. Supóngase, específicamente, que f es una función de un conjunto X al mismo conjunto X, y supóngase que a es un elemento de X. Parece natural el tratar de definir una sucesión infinita $\{u(n)\}$ de elementos de X (esto es, una función u de ω a X) en una forma tal como ésta: escríbase $u(0) = a$, $u(1) = f[u(0)]$, $u(2) = f[u(1)]$, y así sucesivamente. Si el que supuestamente define fuese presionado a explicar el "así sucesivamente" podría recurrir a la inducción. Todo lo que significa, diría, es que definimos $u(0)$ como a, y entonces, inductivamente, definimos $u(n^+)$ como $f[u(n)]$ para todo n. Esto puede parecer factible, pero como justificación para una afirmación de existencia, es insuficiente. El principio de inducción matemática demuestra de hecho, fácilmente, que puede haber cuando mucho una función que satisfaga todas las condiciones propuestas, pero no establece la *existencia* de tal función. Lo que se necesita es el siguiente resultado.

Teorema de inducción. *Si a es un elemento de un conjunto X, y f una función de X en X, entonces existe una función u de ω en X tal que $u(0) = a$ y que $u(n^+) = f[u(n)]$ para todo n de ω.*

Demostración. Recúerdese que una función de ω a X es una cierta clase de subconjunto de $\omega \times X$; construiremos u explícitamente como un conjunto de parejas ordenadas. Considérese, para este objeto, la colección $\mathcal{C}$ de todos aquellos subconjuntos A de $\omega \times X$ para los cuales $(0, a) \in A$ y $[n^+, f(x)] \in A$ siempre que $(n, x) \in A$. Como $\omega \times X$ tiene estas propiedades, la colección $\mathcal{C}$ no es vacía. Entonces, podemos formar la intersección u de todos los conjuntos de la colección $\mathcal{C}$. Como es fácil ver que u mismo pertenece a $\mathcal{C}$, sólo resta demostrar que u es una función. En otras palabras, tenemos que demostrar que para cada número natural n existe cuando mucho un elemento x de X tal que $(n, x) \in u$. (Explícitamente: si tanto (n, x) como (n, y) pertenecen a u, entonces $x = y$). La demostración es inductiva. Sea S el conjunto de todos aquellos números naturales n para los cuales es cierto que $(n, x) \in u$ cuando más para un x. Demostremos que $0 \in S$ y que si $n \in S$, entonces $n^+ \in S$.

¿Pertenece 0 a S? Si no es así, entonces $(0, b) \in u$ para algún b distinto de a. Considérese, en este caso, al conjunto $u - \{(0, b)\}$. Obsérvese que este conjunto disminuido sigue conteniendo a $(0, a)$ (ya que $a \neq b$), y que si el conjunto disminuido contiene a (n, x), entonces contiene también a $[n^+, f(x)]$. La razón para la segunda afirmación es que como $n^+ \neq 0$, el elemento descartado no es igual a $[n^+, f(x)]$. En otras palabras, $u - \{(0, b)\} \in \mathcal{C}$. Esto contradice al hecho de que u es el conjunto más pequeño de $\mathcal{C}$, y debemos concluir entonces que $0 \in S$.

Supóngase ahora que $n \in S$; esto significa que existe un único elemento x en X tal que $(n, x \in u$. Como $(n, x) \in u$, se sigue que $[n^+, f(x)] \in u$. Si n^+ no pertenece a S, entonces $(n^+, y) \in u$ para algún y diferente de $f(x)$. Considérese, en este caso, al conjunto $u - \{(n^+, y)\}$. Obsérvese que este conjunto disminuido contiene a $(0, a)$ (ya que $n^+ \neq 0$), y que si el conjunto disminuido contiene a (m, t), digamos, entonces contiene también a $[m^+, f(t)]$. En realidad, si $m = n$, entonces t debe ser x, y la razón de que el conjunto disminuido contenga a $[n^+, f(x)]$ es que

$f(x) \neq y$; si, por otra parte, $m \neq n$, entonces la razón de que el conjunto disminuido contenga a $[m^+, f(t)]$ es que $m^+ \neq n^+$. En otras palabras, $u - \{(n^+, y)\} \in \mathcal{C}$. Esto nuevamente contradice al hecho de que u es el conjunto más pequeño de $\mathcal{C}$, y entonces debemos concluir que $n^+ \in S$.

La demostración del teorema de inducción está completa. Una aplicación del mismo es conocida como *definición por inducción.*

EJERCICIO. Demuestre que si n es un número natural, entonces $n \neq n^+$; si $n \neq 0$, entonces $n = m^+$ para algún número natural m. Demuestre que ω es transitivo. Demuestre que si E es un subconjunto no vacío de algún número natural, entonces existe un elemento k en E tal que $k \in m$ siempre que m sea un elemento de E distinto de k.

SECCION 13

ARITMETICA

La introducción de la adición para los números naturales es un ejemplo típico de definición por inducción. En efecto, del teorema de inducción se sigue que para cada número natural m existe una función s_m de ω a ω tal que $s_m(0) = m$ y tal que $s_m(n^+) = [s_m(n)]^+$ para cada número natural n; el valor $s_m(n)$ es, por definición, la *suma* $m + n$. Las propiedades aritméticas generales de la adición son demostradas mediante aplicaciones repetidas del principio de inducción matemática. Así por ejemplo, la adición es asociativa. Esto significa que

$$(k + m) + n = k + (m + n)$$

siempre que k, m y n sean números naturales. La demostración se hace por inducción sobre n de la manera siguiente. Como $(k + m) + 0 = k + m$ y $k + (m + 0) = k + m$, la ecuación es cierta si $n = 0$. Si la ecuación es cierta para n, entonces $(k + m) + n^+ = [(k + m) + n]^+$ (por definición) $= [k + (m + n)]^+$ (por la hipótesis de inducción) $= k + (m + n)^+$ (otra vez por la definición de adición) $= k + (m + n^+)$ (ídem), lo cual completa la demostración. Para demostrar que la adición es conmutativa (esto es, que $m + n = n + m$ para todo m y todo n) se necesitan ciertos artificios; un ataque directo podría fallar. El artificio consiste en demostrar, por inducción sobre n, que (i) $0 + n = n$ y que (ii) $m^+ + n = (m + n)^+$, y demostrar después la ecuación de conmutatividad deseada por inducción sobre m, vía (i) y (ii).

Técnicas semejantes son aplicadas en las definiciones de productos y exponentes así como en la derivación de sus pro-

piedades aritméticas fundamentales. Para definir la multiplicación, aplíquese el teorema de inducción para producir las funciones p_m tales que $p_m(0) = 0$ y que $p_m(n^+) = p_m(n) + m$ para cada número natural n; el valor $p_m(n)$ es entonces, por definición, el *producto* $m \cdot n$. (Frecuentemente es omitido el punto). La multiplicación es asociativa y conmutativa; las demostraciones son adaptaciones directas de las que se realizaron en la adición. La ley distributiva (o sea, la afirmación de que $k \cdot (m + n) = k \cdot m + k \cdot n$ siempre que k, m y n sean números naturales) es otra consecuencia sencilla del principio de inducción matemática. (Empléese inducción sobre n.) Cualquiera que haya procedido de esta manera en las sumas y los productos no debe tener dificultad con los exponentes. El teorema de inducción produce funciones e_m tales que $e_m(0) = 1$ y que $e_m(n^+) = e_m(n) \cdot m$ para cada número natural n; el valor $e_m(n)$ es, por definición, la *potencia* m^n. La deducción y el establecimiento de las propiedades de las potencias, así como las demostraciones detalladas de las proposiciones relativas a productos, pueden quedar como ejercicios para el lector sin peligro alguno.

El siguiente tema que merece cierta atención es la teoría del orden en el conjunto de los números naturales. Con este fin, procederemos a examinar con algún cuidado lo referente a cuáles números naturales pertenecen a cuáles otros. Formalmente, decimos que dos números naturales m y n son comparables si $m \in n$, o $m = n$, o $n \in m$. Afirmación: dos números naturales son siempre comparables. La demostración de esta afirmación consta de varios pasos; será conveniente introducir alguna notación. Para cada n en ω, escríbase $S(n)$ para el conjunto de todos los m de ω que son comparables con n, y sea S el conjunto de todos aquellos n para los cuales $S(n) = \omega$. En esos términos, la proposición es que $S = \omega$. Comenzaremos la demostración haciendo ver que $S(0) = \omega$ (esto es, que $0 \in S$). Evidentemente, $S(0)$ contiene a 0. Si $m \in S(0)$, entonces, como es imposible que $m \in 0$, deberá tenerse $m = 0$ (en cuyo caso $0 \in m^+$) o bien $0 \in m$ (en cuyo caso, otra vez, $0 \in m^+$). Así, en todos los casos, si $m \in S(0)$, entonces $m^+ \in S(0)$, lo cual demuestra que $S(0) = \omega$. La demostración quedará completa haciendo ver que si $S(n) = \omega$, entonces $S(n^+) = \omega$. El hecho de que $0 \in S(n^+)$ es inmediato [ya que $n^+ \in S(0)$]; que-

da por demostrar que si $m \in S(n^+)$, entonces $m^+ \in S(n^+)$. Como $m \in S(n^+)$ deberá tenerse que $n^+ \in m$ (en cuyo caso $n^+ \in m^+$), o que $n^+ = m$ (*ídem*), o que $m \in n^+$. En el último caso, o $m = n$ (en cuyo caso $m^+ = n^+$), o $m \in n$. El último caso, en turno, se descompone de acuerdo con el comportamiento de m^+ y de n: puesto que $m^+ \in S(n)$, deberemos tener ya sea $n \in m^+$, o $n = m^+$, o $m^+ \in n$. La primera posibilidad es incompatible con la presente situación (o sea, con $m \in n$). La razón es que si $n \in m^+$, entonces $n \in m$ o $n = m$, de modo que, en cualquier caso, $n \subset m$, y sabemos que ningún número natural es un subconjunto de uno de sus elementos. Las dos posibilidades restantes implican que $m^+ \in n^+$, lo cual completa la demostración.

El párrafo precedente implica que si m y n están en ω, entonces cuando menos una de las tres posibilidades ($m \in n$, $m = n$, $n \in m$) debe cumplirse; es fácil ver que siempre se cumple exactamente una de las tres. (La razón es otra aplicación del hecho de que un número natural no es un subconjunto de uno de sus elementos.) Otra consecuencia del párrafo precedente es que si n y m son números naturales distintos entre sí, entonces una condición necesaria y suficiente para que $m \in n$ es que $m \subset n$. En realidad, el hecho de que $m \in n$ implique que $m \subset n$ no es más que la transitividad de n. *Si*, recíprocamente, $m \subset n$ y $m \neq n$, entonces $n \in m$ no puede ser cierto ya que entonces m sería un subconjunto de uno de sus elementos), por lo tanto, $m \in n$. Si $m \in n$ o equivalentemente si m es un subconjunto propio de n, escribiremos $m < n$ y diremos que m es *menor* que n. Si se sabe que m es menor que, o igual a n, escribiremos $m \leqq n$. Obsérvese que $\leqq$ y $<$ son relaciones en ω. La primera es reflexiva, pero la última no lo es; ninguna es simétrica y ambas son transitivas. Si $m \leqq n$ y $n \leqq m$, entonces $m = n$.

EJERCICIO. Demuestre que si $m < n$, entonces $m + k < n + k$ y que si $m < n$ y $k \neq 0$, entonces $m \cdot k < n \cdot k$. Demuestre que si E es un conjunto no vacío de números naturales, entonces existe un elemento k en E tal que $k \leqq m$ para toda m en E.

Se dice que dos conjuntos E y F (no necesariamente subconjuntos de ω) son *equivalentes*, en símbolos $E \sim F$, si existe una correspondencia uno a uno* entre ellos. Es fácil verificar que, para subconjuntos de un conjunto particular X, la equi-

* Véase nota en la Pág. 50. (N. del R.)

valencia en este sentido es una relación de equivalencia en el conjunto potencia $\mathcal{P}(X)$.

Cualquier subconjunto propio de un número natural n es equivalente a algún número natural más pequeño (esto es, a algún elemento de n). La demostración de esta afirmación es inductiva. Para $n = 0$ es trivial. Si es cierta para n y si E es un subconjunto propio de n^+, entonces o E es un subconjunto propio de n y se aplica la hipótesis de inducción, o $E = n$ y el resultado es trivial, o $n \in E$. En el último caso, encuéntrese un número k que esté en n pero no en E y defínase una función f en E escribiendo $f(i) = i$ cuando $i \neq n$ y $f(n) = k$. Es claro que f es uno a uno y que transforma a E en n. Se sigue que la imagen de E bajo f es igual a n o (por la hipótesis de inducción) equivalente a algún elemento de n, y, consecuentemente, E mismo siempre es equivalente a algún elemento de n^+.

Es un hecho ligeramente molesto que un conjunto pueda ser equivalente a un subconjunto propio de sí mismo. Si, por ejemplo, se define una función f de ω a ω escribiendo $f(n) = n^+$ para todo n de ω, entonces f es una correspondencia uno a uno entre el conjunto de todos los números naturales y el subconjunto propio constituido por los números naturales distintos de cero. Es agradable saber que aunque el conjunto de todos los números naturales tiene esta propiedad peculiar, la cordura prevalece para cada número natural particular. En otras palabras, si $n \in \omega$, entonces n no es equivalente a un subconjunto propio de n. Esto es claro para $n = 0$. Supóngase ahora que es cierto para n y que f es una correspondencia uno o uno de n^+ a un subconjunto propio E de n^+. Si $n \epsilon' E$, entonces la restricción de f a n es una correspondencia uno a uno entre n y un subconjunto propio de n, lo cual contradice a la hipótesis de inducción. Si $n \in E$, entonces n es equivalente a $E - \{n\}$, de manera que, por la hipótesis de inducción, $n = E - \{n\}$. Esto implica que $E = n^+$, lo cual contradice la suposición de que E es un subconjunto propio de n^+.

Un conjunto E es llamado *finito* si es equivalente a algún número natural; de otra manera E es *infinito*.

EJERCICIO. Use esta definición para demostrar que ω es infinito.

Un conjunto puede ser equivalente a lo más a un número natural. (Demostracion: sabemos que para cada dos

números naturales distintos entre sí uno debe ser un elemento y, por lo tanto, un subconjunto propio del otro; se sigue del párrafo precedente que no pueden ser equivalentes.) Podemos inferir que un conjunto finito nunca es equivalente a un subconjunto propio; en otras palabras, mientras nos limitemos a conjuntos finitos, el todo es siempre mayor que cualquiera de sus partes.

EJERCICIO. Use esta consecuencia de la definición de finito para demostrar que ω es infinito.

Ya que todo subconjunto de un número natural es equivalente a un número natural, se sigue también que todo subconjunto de un conjunto finito es finito.

El *número de elementos* en un conjunto finito E es, por definición, el único número natural equivalente a E y lo denotaremos por $\#(E)$. Es claro que si la correspondencia entre E y $\#(E)$ es restringuida a los subconjuntos finitos de algún conjunto X, el resultado es una función de un subconjunto del conjunto potencia $\mathcal{P}(X)$ a ω. Esta función está agradablemente relacionada con las operaciones y relaciones familiares de la teoría de los conjuntos. Así, por ejemplo, si E y F son dos conjuntos finitos tales que $E \subset F$, entonces $\#(E) \leqq \#(F)$. [La razón es que como $E \sim \#(E)$ y $F \sim \#(F)$, se sigue que $\#(E)$ es equivalente a un subconjunto de $\#(F)$]. Otro ejemplo, es la afirmación de que si E y F son conjuntos finitos, entonces $E \cup F$ es finito y más aún, si E y F son ajenos, entonces $\#(E \cup F) = \#(E) + \#(F)$. El paso crucial de la demostración es el hecho de que si m y n son números naturales, entonces el complemento de m en la suma $m + n$ es equivalente a n; la demostración de este hecho auxiliar se consigue por inducción sobre n. Con técnicas semejantes se demuestra que si E y F son dos conjuntos finitos, entonces también lo son $E \times F$ y E^F, y, más aún, $\#(E \times F) = \#(E) \cdot \#(F)$ y $\#(E^F) = \#(E)^{\#(F)}$.

EJERCICIO. La unión de un conjunto finito de conjuntos finitos es finita. Si E es finito entones $\mathcal{P}(E)$ es finito y, más aún, $\#[\mathcal{P}(E)] = 2^{\#(E)}$. Si E es un conjunto finito no vacío de números naturales, entonces existe un elemento k en E tal que $m \leqq k$ para todo m en E.

SECCION 14

ORDEN

La teoría del orden tiene un importante papel a lo largo de las matemáticas y, en particular, en la generalización a conjuntos infinitos del proceso de contar apropiado para conjuntos finitos. Las definiciones básicas son simples. Lo único que hay que recordar es que la motivación original viene de las propiedades familiares de "menor que o igual a" y no "menor que". No hay ninguna razón profunda para esto; sucede simplemente que la generalización de "menor que o igual a" ocurre más frecuentemente y es más adecuada para un tratamiento algebraico.

Una relación R en un conjunto X es llamada *antisimétrica* si para cada x y cada y en X, la validez simultánea de $x\,R\,y$ y $y\,R\,x$ implica que $x = y$. Un *orden parcial* (o algunas veces simplemente un *orden*) en un conjunto X es una relación en X que es reflexiva, antisimétrica y transitiva. Se acostumbra usar sólo un símbolo (o algo tipográficamente muy parecido a él) para la mayoría de los órdenes parciales en la mayoría de los conjuntos; el símbolo en uso común es el familiar signo de desigualdad. Así, un orden parcial en X puede ser definido como una relación $\leqq$ en X tal que, para todo x, y y z en X, se tenga (i) $x \leqq x$, (ii) si $x \leqq y$ y $y \leqq x$, entonces $x = y$, y (iii) si $x \leqq y$ y $y \leqq z$, entonces $x \leqq z$. La razón del calificativo "parcial" es que algunas preguntas acerca del orden pueden dejarse sin respuesta. Si para todo x y y en X se tiene $x \leqq y$ o $y \leqq x$, entonces $\leqq$ es llamado *orden total* (algunas veces también se le llama orden *simple o lineal*). Un conjunto totalmente ordenado recibe con frecuencia el nombre de *cadena*.

EJERCICIO. Exprese las condiciones de antisimetría y totalidad para una relación R en términos de ecuaciones que involucren a R y a su inversa.

El ejemplo más natural de un orden parcial (y no total) es la inclusión. Explícitamente: para cada conjunto X, la relación $\subset$ es un orden parcial en el conjunto potencia $\mathcal{P}(X)$; es un orden total si y sólo si X es vacío o es un conjunto singular. Un ejemplo bien conocido de orden total es la relación "menor que o igual a" en el conjunto de los números naturales. Un orden parcial interesante y frecuentemente visto es la relación de extensión para funciones. Explícitamente: para conjuntos dados X y Y, sea F el conjunto de todas aquellas funciones cuyo dominio está incluido en X y cuyo rango está incluido en Y. Defina una relación R en F escribiendo $f\ R\ g$ siempre que dom $f \subset$ dom g y $f(x) = g(x)$ para todo x en dom f; en otras palabras, $f\ R\ g$ significa que f es una restricción de g, o, equivalentemente, que g es una extensión de f. Si recordamos que las funciones en F son, después de todo, ciertos subconjuntos del producto cartesiano $X \times Y$, advertiremos que $f\ R\ g$ significa que $f \subset g$; la extensión es un caso especial de la inclusión.

Un *conjunto parcialmente ordenado* es un conjunto junto con un orden parcial en él. Una formulación precisa de este "junto" es la siguiente: un conjunto parcialmente ordenado es una pareja ordenada $(X, \leqq)$, donde X es un conjunto y $\leqq$ es un orden parcial en X. Esta clase de definición es muy común en las matemáticas; una estructura matemática es casi siempre un conjunto "junto" con otros conjuntos, funciones y relaciones especificadas. La manera aceptada de hacer que esas definiciones sean precisas es por referencia a parejas ordenadas, ternas o cualquier cosa que sea apropiada. Esa no es la única manera. Obsérvese por ejemplo, que el conocimiento de un orden parcial implica el conocimiento de su dominio. Por consiguiente, si describimos un conjunto parcialmente ordenado como una pareja ordenada, estamos siendo un tanto redundantes, pues la segunda coordenada sola habría comunicado la misma cantidad de información. Sin embargo, en cuestiones de lenguaje y notación, la tradición siempre vence a la razón pura. El comportamiento matemático aceptado (para estructuras en general e ilustrado aquí para conjuntos parcialmente ordenados) es el de admitir que las parejas ordenadas son la vía de entrada correcta, olvidar que la segunda coordenada es

la importante y hablar como si la primera coordenada fuese todo lo que interesara. Siguiendo la costumbre, a menudo diremos algo como "sea X un conjunto parcialmente ordenado", cuando lo que realmente queremos decir es "sea X el dominio de un orden parcial". Las mismas convenciones linguísticas se aplican a conjuntos totalmente ordenados, o sea, a conjuntos parcialmente ordenados cuyo orden es de hecho total.

La teoría de los conjuntos parcialmente ordenados emplea muchas palabras cuyo significado técnico es tan cercano a su interpretación corriente que prácticamente son autoexplicativas. Para ser concretos, supóngase que X es un conjunto parcialmente ordenado y que x y y son elementos de X. Escribiremos $y \geqq x$ en caso de que $x \leqq y$; en otras palabras, $\geqq$ es la inversa de la relación $\leqq$. Si $x \leqq y$ y $x \neq y$ escribiremos $x < y$ y diremos que x es *menor* que, o *más chico* que y, o que x es un *predecesor* de y. Alternativamente, bajo las mismas circunstancias, escribiremos $y > x$ y diremos que y es *mayor* o *más grande* que x, o que y es un *sucesor* de x. La relación $<$ es tal que (i) no hay elementos x y y para los cuales $x < y$ y $y < x$ se cumplan simultáneamente, y (ii) si $x < y$ y $y < z$, entonces $x < z$ (o sea, que $<$ es transitiva). Si, recíprocamente, $<$ es una relación en X que satisface (i) y (ii), y si $x \leqq y$ está definida de manera que signifique $x < y$ o $x = y$, entonces $\leqq$ es un orden parcial en X.

La conexión entre $\leqq$ y $<$ puede ser generalizada a relaciones arbitrarias. Esto es, que dada una relación R en un conjunto X, podemos definir una relación S en X escribiendo $x \, S \, y$ en caso que $x \, R \, y$ pero $x \neq y$, y, viceversa, dada cualquier relación S en X, podemos definir una relación R en X escribiendo $x \, R \, y$ en caso de que $x \, S \, y$ o $x = y$. Con el fin de tener una forma abreviada para referirnos al paso de R a S y viceversa, diremos que S es la relación *estricta* correspondiente a R y que R es la relación *débil* correspondiente a S. Diremos que una relación en un conjunto X "ordena parcialmente a X" cuando la relación es un orden parcial en X o bien cuando lo es la relación débil correspondiente.

Si X es un conjunto parcialmente ordenado y si $a \in X$, el conjunto $\{x \in X : x < a\}$ es el *segmento inicial* determinado por a y lo denotaremos usualmente por $s(a)$. El conjunto $\{x \in X : x \leqq a\}$ es el *segmento inicial débil* determinado por a, y será denotado por $\bar{s}(a)$. Cuando es importante enfatizar la distin-

ción entre segmentos iniciales y segmentos iniciales débiles, los primeros serán llamados segmentos iniciales *estrictos*. En general, las palabras "estricto" y "débil" se refieren a $<$ y $\leqq$ respectivamente. Así, por ejemplo, el segmento inicial determinado por a puede ser descrito como el conjunto de todos los *predecesores* de a, o, para enfatizar, como el conjunto de todos los predecesores *estrictos* de a; análogamente, el segmento inicial débil determinado por a consiste de todos los *predecesores débiles* de a. Si $x \leqq y$ y $y \leqq z$, podemos decir que y está *entre* x y z; si $x < y$ y $y < z$, entonces y *está estrictamente entre* x y z. Si $x < y$ y no hay ningún elemento estrictamente entre x y y, decimos que x es un *predecesor* inmediato de y, o que y es un *sucesor inmediato* de x.

Si X es un conjunto parcialmente ordenado (que puede, en particular, estar totalmente ordenado), entonces puede suceder que X tenga un elemento a tal que $a \leqq x$ para todo x en X. En tal caso decimos que a es *el menor* elemento (*el más chico, el primero*) de X. La antisimetría de un orden implica que si X tiene un menor elemento, éste es único. Si, análogamente X tiene un elemento a tal que $x \leqq a$ para todo x en X, entonces a es *el mayor* elemento (*el más grande, el último*) de X; éste también es único (si es que existe). El conjunto ω de todos los números naturales (con su ordenamiento por magnitud acostumbrado) es un ejemplo de conjunto parcialmente ordenado con un primer elemento (a saber, 0) pero sin un último. El mismo conjunto, pero esta vez con el ordenamiento inverso, tiene un último elemento, pero no un primero.

En conjuntos parcialmente ordenados hay una importante diferencia entre menores elementos y elementos mínimos. Si, como antes, X es un conjunto parcialmente ordenado, un elemento a de X es llamado elemento *mínimo* de X en caso de que no haya en X un elemento estrictamente menor que a. Equivalentemente, a es mínimo si $x \leqq a$ implica que $x = a$. Como ejemplo, considérese a la colección $\mathcal{C}$ de subconjuntos no vacíos de un conjunto no vacío X, con ordenamiento por inclusión. Cada conjunto singular es un elemento mínimo de $\mathcal{C}$, pero es claro que $\mathcal{C}$, no tiene un primer elemento (a menos que X mismo sea un conjunto singular). En forma semejante distinguimos mayores elementos de elementos máximos; un elemento *máximo* de X es un elemento a tal que X no contiene

nada estrictamente mayor que a. Equivalentemente, a es un máximo si $a \leqq x$ implica que $x = a$.

Se dice que un elemento a de un conjunto parcialmente ordenado es una *cota inferior* de un subconjunto E de X en caso de que $a \leqq x$ para todo x en E; análogamente, a es una *cota superior* de E en caso de que $x \leqq a$ para todo x en E. Es posible que un conjunto E no tenga cotas superiores ni inferiores, o que tenga muchas; en el último caso puede suceder que ninguna de ellas pertenezca a E. (¿Ejemplos?) Sea E_* el conjunto de todas las cotas inferiores de E en X y sea E^* el conjunto de todas las cotas superiores de E en X. Lo que se acaba de decir es que E_* puede ser vacío, o que $E_* \cap E$ puede ser vacío. Si $E_* \cap E$ no es vacío, entonces es un conjuno singular constituido por el único primer elemento de E. Por supuesto que observaciones semejantes son aplicables a E^*. Si sucede que el conjunto E_* contiene un mayor elemento a (necesariamente único), entonces a es conocido como la *mayor cota inferior*† *o el ínfimo* de E. Las abreviaciones *m.c.i.* e *inf* son de uso común. A causa de las dificultades para pronunciar la primera, e incluso para recordar sí m.c.i. está arriba (mayor) o está abajo (inferior), usaremos solamente la última notación. Así, inf E es el único elemento en X (posiblemente no en E) que es una cota inferior de E y que domina (es decir, que es mayor que) cualquier otra cota inferior de E. Las definiciones en el otro extremo son completamente análogas. Si E^* tiene un menor elemento a (necesariamente único), entonces a es conocido como la *menor cota superior* (m.c.s.) o *supremo* (sup) de E.

Las ideas conectadas con conjuntos parcialmente ordenados son fáciles de expresar pero toma algún tiempo asimilarlas. Se aconseja al lector que elabore muchos ejemplos para ilustrar las diversas posibilidades en el comportamiento de los conjuntos parcialmente ordenados y sus subconjuntos. Con el fin de auxiliarlo en esta empresa, procederemos a describir tres conjuntos parcialmente ordenados especiales con ciertas propiedades divertidas. (i) El conjunto es $\omega \times \omega$. Para eliminar cualquier confusión posible, denotaremos el orden que vamos a introducir mediante el símbolo neutral R. Si (a, b) y (x, y) son dos parejas ordenadas de números naturales, entonces $(a, b)\ R\ (x, y)$ significa, por definición, que $(2a + 1) \cdot 2^y$

† Suele decirse "máxima cota inferior" porque en el caso de orden total *máximo* y mayor coinciden y en textos comunes sólo aparecen ordenamientos totales. (N. del R.)

$\leqq (2x+1) \cdot 2^b$. (Aquí el signo de desigualdad se refiere al ordenamiento acostumbrado de los números naturales.) El lector que esté dispuesto a dar un salto en el desarrollo lógico reconocerá que, exceptuando la notación, lo que acabamos de definir es el orden usual para $\frac{2a+1}{2^b}$ y $\frac{2x+1}{2^y}$. (ii) El conjunto es otra vez $\omega \times \omega$. Nuevamente usaremos un símbolo neutral para el orden; digamos S. Si (a, b) y (x, y) son parejas ordenadas de números naturales, entonces $(a, b)\, S\, (x, y)$ significa, por definición, que a es estrictamente menor que x (en el sentido acostumbrado), o bien, que $a = x$ y $b \leqq y$. A causa de su semejanza con la forma en que las palabras están dispuestas en un diccionario, a éste se le llama orden *lexicográfico* de $\omega \times \omega$. (iii) Una vez más el conjunto es $\omega \times \omega$. La relación de orden actual, digamos T, es tal que $(a, b)\, T\, (x, y)$ significa, por definición, que $a \leqq x$ y $b \leqq y$.

SECCION 15

EL AXIOMA DE LA ELECCION

Para los resultados más profundos acerca de conjuntos parcialmente ordenados necesitamos una nueva herramienta de la teoría de los conjuntos; interrumpiremos el desarrollo de la teoría del orden el tiempo necesario para obtener esa herramienta.

Comenzaremos obesrvando que un conjunto o es vacío o no lo es, y, si no lo es, entonces, por la definición del conjunto vacío, hay un elemento en él. Esta observación puede ser generalizada. Si X y Y son conjuntos y uno de ellos es vacío, entonces el producto cartesiano $X \times Y$ es vacío. Si ni X ni Y son vacíos, entonces hay un elemento x en X y un elemento y en Y; se sigue que la pareja ordenada (x, y) pertenece al producto cartesiano $X \times Y$, de manera que $X \times Y$ no es vacío. Las observaciones precedentes constituyen los casos $n = 1$ y $n = 2$ de la siguiente afirmación: si $\{X_i\}$ es una sucesión finita de conjuntos, para i en n, digamos, entonces una condición necesaria y suficiente para que su producto cartesiano sea vacío es que cuando menos uno de ellos lo sea. La afirmación se demuestra fácilmente por inducción sobre n. (El caso $n = 0$ conduce a un escurridizo argumento acerca de la función vacía y el lector que no esté interesado puede comenzar la inducción en 1 en vez de 0.)

La generalización a familias infinitas de la parte no trivial de la afirmación del párrafo precedente (la necesidad) es el siguiente importante principio de la teoría de los conjuntos.

Axioma de la elección. *El producto cartesiano de una familia no vacía de conjuntos no vacíos es no vacío.*

En otras palabras: si $\{X_i\}$ es una familia de conjuntos no vacíos con índices en I no vacío, entonces existe una familia $\{x_i\}$, $i \in I$, tal que $x_i \in X_i$ para cada i de I.

Supóngase que $\mathcal{C}$ es una colección no vacía de conjuntos no vacíos. Podemos considerar a $\mathcal{C}$ como una familia, o, para decirlo mejor, podemos convertir a $\mathcal{C}$ en un conjunto "indicado" usando precisamente a la colección $\mathcal{C}$ misma en el papel del conjunto de índices y tomando la función identidad sobre $\mathcal{C}$ en el papel de la "indicación". El axioma de la elección dice entonces que el producto cartesiano de los conjuntos de $\mathcal{C}$ tiene cuando menos un elemento. Un elemento de tal producto cartesiano es, por definición, una función (familia, "conjunto indicado") cuyo dominio es el conjunto de índices (en este caso $\mathcal{C}$) y cuyo valor para cada índice pertenece al conjunto que lleva ese índice. Conclusión: existe una función f con dominio $\mathcal{C}$ tal que si $A \in \mathcal{C}$, entonces $f(A) \in A$. Esta conclusión se aplica, en particular, en el caso en que $\mathcal{C}$ es la colección de todos los subconjuntos no vacíos de un conjunto no vacío X. La afirmación en este caso es que existe una función f con dominio $\mathcal{P}(X) - \{\varnothing\}$ tal que si A está en ese dominio, entonces $f(A) \in A$. En lenguaje intuitivo la función f puede ser descrita como una elección simultánea de un elemento de cada uno de muchos conjuntos; a esto se debe el nombre del axioma. (Una función que en este sentido "elige" un elemento de cada subconjunto no vacío de un conjunto X es conocida como una *función de elección* para X.) Hemos visto que si la colección de conjuntos en la que estamos eligiendo es finita, entonces la posibilidad de elección simultánea es una sencilla consecuencia de lo que sabíamos antes de que el axioma de la elección fuese propuesto; el papel del axioma es el de garantizar esa posibilidad en casos infinitos.

Las dos consecuencias del axioma de la elección en el párrafo precedente (una para el conjunto potencia de un conjunto y la otra para colecciones más generales de conjuntos) son en realidad simples reformulaciones de dicho axioma. Para cada consecuencia del axioma de la elección, solía ser importante examinar hasta qué punto es necesario el axioma en la demostración de la consecuencia. Una demostración alternativa sin el axioma de la elección significaba un triunfo; una demostración recíproca, que hiciera ver que la consecuencia es equivalente al axioma de la elección (en presencia de los axiomas res-

* Conjunto "indicado" = conjunto con índices. (N. del R.)

tantes de la teoría de los conjuntos) significaba una honrosa derrota. Cualquier cosa intermedia se consideraba exasperante. Como una muestra (y ejercicio) tenemos la afirmación de que toda relación incluye una función con el mismo dominio. Otra muestra: si $\mathcal{C}$ es una colección de conjuntos no vacíos ajenos por parejas, entonces existe un conjunto A tal que $A \cap C$ es un conjunto singular para cada C de $\mathcal{C}$. Ambas afirmaciones están entre las muchas que se sabe son equivalentes al axioma de la elección.

Como una ilustración del empleo del axioma de la elección, considérese la afirmación de que si un conjunto es infinito, entonces tiene un subconjunto equivalente a ω. Un argumento informal podría ser el siguiente. Si X es infinito, entonces, en particular, no es vacío (esto es, que no es equivalente a 0); luego, tiene un elemento, digamos x_0. Como X no es equivalente a 1, el conjunto $X - \{x_0\}$ no es vacío y, por lo tanto, tiene un elemento, digamos x_1. Repítase este argumento hasta el infinito; el siguiente paso, por ejemplo, consiste en decir que $X - \{x_0, x_1\}$ no es vacío y, por lo tanto, tiene un elemento, digamos, x_2. El resultado es una sucesión infinita $\{x_n\}$ de elementos distintos de X, que es lo que se quería demostrar. Este bosquejo de demostración tiene cuando menos la virtud de ser honesto respecto a la idea más importante que hay tras él; el acto de elegir un elemento de un conjunto no vacío fue repetido infinitamente. El matemático experimentado en los métodos del axioma de la elección ofrecerá a menudo tal argumento informal; su experiencia le permite ver fácilmente cómo hacerlo preciso. Para nuestros propósitos es aconsejable ver las cosas más detalladamente.

Sea f una función de elección para X; esto es, f es una función de la colección de todos los subconjuntos no vacíos de X con valores en X tal que $f(A) \in A$ para todo A del dominio de f. Sea $\mathcal{C}$ la colección de todos los subconjuntos finitos de X. Como X es infinito, se sigue que si $A \in \mathcal{C}$, entonces $X - A$ no es vacío, y por consiguiente $X - A$ pertenece al dominio de f. Defínase una función g de $\mathcal{C}$ a $\mathcal{C}$ escribiendo $g(A) = A \cup \{f(X - A)\}$. En palabras: $g(A)$ se obtiene agregando a A el elemento que f elige de $X - A$. Aplicamos el teorema de inducción a la función g; podemos empezar, por ejemplo, con el conjunto $\varnothing$. El resultado es que existe una función U de ω a $\mathcal{C}$ tal que $U(0) = \varnothing$ y $U(n^+) = U(n) \cup \{f[X - U(n)]\}$ para cada número

demostración de *

natural n. Afirmación: si $v(n) = f[X - U(n)]$, entonces v es una correspondencia uno a uno de ω a X, por lo cual, en realidad, ω es equivalente a algún subconjunto de X, (a saber, el rango de v). Para demostrar esta afirmación, haremos una serie de observaciones elementales; sus demostraciones son sencillas consecuencias de las definiciones. Primera: $v(n) \epsilon' U(n)$ para todo n. Segunda: $v(n) \epsilon U(n^+)$ para todo n. Tercera: si n y m son números naturales y $n \leqq m$, entonces $U(n) \subset U(m)$. Cuarta: si n y m son números naturales y $n < m$, entonces $v(n) \neq v(m)$. [Razón: $v(n) \epsilon U(m)$ pero $v(m) \epsilon' U(m)$]. La última observación implica que v transforma números naturales distintos en elementos distintos de X y todo lo que tenemos que recordar es que de cada dos números naturales distintos cualesquiera uno es estrictamente menor que el otro.

La demostración está completa; ahora sabemos que cualquier conjunto infinito tiene un subconjunto equivalente a ω. Este resultado, demostrado aquí no tanto por su interés intrínseco como por dar un ejemplo del uso adecuado del axioma de la elección, tiene un interesante corolario. La afirmación es que un conjunto es infinito si y sólo si es equivalente a un subconjunto propio de sí mismo. La parte "si" ya la conocemos; dice tan sólo que un conjunto finito no puede ser equivalente a un subconjunto propio. Para demostrar la parte "sólo si", supóngase que X es infinito y sea v una correspondencia uno a uno de ω hacia X. Si x está en el rango de v, digamos $x = v(n)$, escríbase $h(x) = v(n^+)$; si x no está en el rango de v, escríbase $h(x) = x$. Es fácil verificar que h es una correspondencia uno a uno de X hacia sí mismo. Como el rango de h es un subconjunto propio de X [no contiene a $v(0)$], la demostración del corolario es completa. La afirmación del corolario fue usada por Dedekind como definición misma de infinito.

SECCION 16

LEMA DE ZORN

Un teorema de existencia afirma la existencia de un objeto perteneciente a cierto conjunto y poseedor de ciertas propiedades. Muchos teoremas de existencia pueden ser formulados (o, si es necesario, reformulados) de manera que el conjunto subyacente sea un conjunto parcialmente ordenado y la propiedad crucial es lo máximo.* Nuestro siguiente propósito es el de enunciar y demostrar el teorema más importante de esta clase.

Lema de Zorn. *Si X es un conjunto parcialmente ordenado tal que toda cadena en X tiene una cota superior, entonces X contiene un elemento máximo.*

DISCUSIÓN. Recuérdese que una cadena es un conjunto totalmente ordenado. Por una cadena "en X" entendemos un subconjunto de X tal que el subconjunto, considerado como un conjunto parcialmente ordenado por derecho propio, resulta estar totalmente ordenado. Si A es una cadena en X, la hipótesis del lema de Zorn garantiza la existencia de una cota superior para A en X; no garantiza la existencia de una cota superior para A en A. La conclusión del lema de Zorn es la existencia de un elemento a en X con la propiedad de que si $a \leqq x$, entonces necesariamente $a = x$.

La idea principal de la demostración es semejante a la que se empleó en nuestro estudio precedente de conjuntos infinitos. Ya que, por hipótesis, X no es vacío, tiene un elemento, digamos x_0. Si x_0 es máximo, deténgase aquí. Si no lo es, entonces existe un elemento, digamos x_1, estrictamente mayor que

* El original dice, literalmente, que la propiedad crucial es "la maximalidad", palabra que no se usa en nuestro idioma. (N. del T.).

x_0. Si x_1 es máximo, deténgase aquí; en caso contrario continúe. Repítase este razonamiento indefinidamente; por último debe conducir a un elemento máximo.

La última oración es probablemente la parte menos convincente de la demostración, ya que esconde multitud de dificultades. Obsérvese, por ejemplo, la siguiente posibilidad. Podría suceder que el razonamiento, repetido indefinidamente, condujera a toda una sucesión infinita de elementos no máximos; ¿qué vamos a hacer en ese caso? La respuesta es que el rango de tal sucesión infinita es una cadena en X, y, consecuentemente, tiene una cota superior; lo que hay que hacer entonces es iniciar otra vez todo el argumento, partiendo de esa cota superior. Lo menos que podemos decir es que el problema de cuándo precisamente y cómo va a llegar todo esto a un final, es oscuro. No hay forma de remediarlo; debemos buscar la demostración precisa. La estructura de dicha demostración es una adaptación de una dada originalmente por Zermelo.

DEMOSTRACIÓN. El primer paso es reemplazar al orden parcial abstracto por el orden de inclusión en una colección adecuada de conjuntos. Más precisamente, consideramos, para cada elemento x de X, el segmento inicial débil $\bar{s}(x)$ constituido por x y sus predecesores. El rango $\mathcal{S}$ de la función $\bar{s}$ [de X a $\mathcal{P}(X)$] es una cierta colección de subconjuntos de X, los cuales, por supuesto, debemos considerar como (parcialmente) ordenados por inclusión. La función $\bar{s}$ es uno a uno, y una condición necesaria y suficiente para que $\bar{s}(x) \subset \bar{s}(y)$ es que $x \leqq y$. En vista de esto, la tarea de encontrar un elemento máximo en X es la misma que la de encontrar un conjunto máximo en $\mathcal{S}$. La hipótesis acerca de las cadenas en X implica (y es, de hecho, equivalente a) la proposición correspondiente acerca de las cadenas en $\mathcal{S}$.

Sea $\mathfrak{X}$ el conjunto de todas las cadenas en X, todo miembro de $\mathfrak{X}$ está incluido en $s(x)$ para algun x de X. La colección $\mathfrak{X}$ es una colección no vacía de conjuntos, parcialmente ordenados por inclusión, y tal que si $\mathcal{C}$ es una cadena en $\mathfrak{X}$, entonces la unión de los conjuntos en $\mathcal{C}$ (o sea $\bigcup_{A \in \mathcal{C}} A$) pertenece a $\mathfrak{X}$. Como cada conjunto de $\mathfrak{X}$ está dominado por algún conjunto de $\mathcal{S}$, el paso de $\mathcal{S}$ a $\mathfrak{X}$ no puede introducir nuevos elementos máximos. Una ventaja de la colección $\mathfrak{X}$ es la

forma ligeramente más específica que toma la hipótesis de la cadena, ya que en lugar de decir que cada cadena $\mathcal{C}$ tiene cierta cota superior en $\mathcal{S}$, podemos decir explícitamente que la unión de los conjuntos de $\mathcal{C}$, la cual es claramente una cota superior de $\mathcal{C}$, es un elemento de la colección $\mathfrak{X}$. Otra ventaja técnica de $\mathfrak{X}$ es que contiene a todos los subconjuntos de cada uno de sus conjuntos, lo cual hace posible aumentar conjuntos no máximos en $\mathfrak{X}$ lentamente, elemento por elemento.

Ahora podemos olvidar el orden parcial dado en X. En lo que sigue consideraremos una colección no vacía $\mathfrak{X}$ de subconjuntos de un conjunto no vacío X, sujeta a dos condiciones: cualquier subconjunto de cada conjunto de $\mathfrak{X}$ está en $\mathfrak{X}$, y la unión de cada cadena de conjuntos en $\mathfrak{X}$ está en $\mathfrak{X}$. Nótese que la primera condición implica que $\varnothing \in \mathfrak{X}$. Nuestra tarea es demostrar que existe un conjunto máximo en $\mathfrak{X}$.

Sea f una función de elección para X, esto es, f es una función de la colección de todos los subconjuntos no vacíos de X con valores en X tal que $f(A) \in A$ para todo A del dominio de f. Para cada conjunto A de $\mathfrak{X}$, sea $\hat{A}$ el conjunto de todos aquellos elementos x de X cuya adjunción a A produce un conjunto en $\mathfrak{X}$; en otras palabras, $\hat{A} = \{x \in X : A \cup \{x\} \in \mathfrak{X}\}$. Defínase una función g de $\mathfrak{X}$ a $\mathfrak{X}$ en la forma siguiente: si $\hat{A} - A \neq \varnothing$, entonces $g(A) = A \cup \{f(\hat{A} - A)\}$; si $\hat{A} - A = \varnothing$, entonces $g(A) = A$. Se sigue de la definición de $\hat{A}$ que $\hat{A} - A = \varnothing$ si y sólo si A es máximo. Por lo tanto, en estos términos, lo que debemos demostrar es que existe en $\mathfrak{X}$ un conjunto A tal que $g(A) = A$. Resulta que la propiedad crucial de g es el hecho de que $g(A)$ (que siempre incluye a A) contiene cuando mucho un elemento más que A.

Ahora, para facilitar la exposición, introduciremos una definición provisional. Diremos que una subcolección $\mathfrak{J}$ de $\mathfrak{X}$ es una *torre si*

(i) $\varnothing \in \mathfrak{J}$,
(ii) *si* $A \in \mathfrak{J}$, *entonces* $g(A) \in \mathfrak{J}$,
(iii) *si* $\mathcal{C}$ *es una cadena en* $\mathfrak{J}$, *entonces* $\bigcup_{A \in \mathcal{C}} A \in \mathfrak{J}$.

Las torres existen de seguro; la colección $\mathfrak{X}$ completa es una. Ya que la intersección de una colección de torres es a su vez una torre, se sigue, en particular, que si $\mathfrak{J}_0$ es la intersección de todas las torres, entonces $\mathfrak{J}_0$ es la torre más chica. Nuestro propósito inmediato es demostrar que la torre $\mathfrak{J}_0$ es una cadena.

Permítasenos decir que unconjunto C de $\mathfrak{J}_0$ es *comparable*

si es comparable con cada conjunto de $\mathfrak{J}_0$; esto significa que si $A \in \mathfrak{J}_0$, entonces $A \subset C$ o $C \subset A$. Decir que $\mathfrak{J}_0$ es una cadena significa que todos los conjuntos en $\mathfrak{J}_0$ son comparables. Los conjuntos comparables existen de seguro; $\varnothing$ es uno de ellos. En los siguientes dos párrafos concentraremos nuestra atención en un conjunto comparable arbitrario pero temporalmente fijo C. Supóngase que $A \in \mathfrak{J}_0$ y que A es un subconjunto propio de C. Afirmación: $g(A) \subset C$. La razón es que como C es comparable, entonces $g(A) \subset C$ o bien C es un subconjunto propio de $g(A)$. En el último caso A es un subconjunto propio de un subconjunto propio de $g(A)$, lo cual contradice el hecho de que $g(A) - A$ no puede ser más que un conjunto singular.

Considérese en seguida la colección $\mathfrak{U}$ de todos aquellos conjuntos A de $\mathfrak{J}_0$ para los cuales se tiene $A \subset C$ o bien $g(C) \subset A$. La colección $\mathfrak{U}$ es un tanto más chica que la colección de conjuntos de $\mathfrak{J}_0$ comparable con $g(C)$; en realidad, si $A \in \mathfrak{U}$, entonces, como $C \subset g(C)$, se tendrá $A \subset g(C)$ o bien $g(C) \subset A$. Afirmación: $\mathfrak{U}$ es una torre. Como $\varnothing \subset C$, la primera condición sobre torres está satisfecha. Para demostrar la segunda, o sea, que si $A \in \mathfrak{U}$, entonces $g(A) \in \mathfrak{U}$, divídase la discusión en tres casos. Primero: A es un subconjunto propio de C. Entonces $g(A) \subset C$ por el párrafo precedente y, por lo tanto, $g(A) \in \mathfrak{U}$. Segundo: $A = C$. Entonces $g(A) = g(C)$, de manera que $g(C) \subset g(A)$ y, por consiguiente, $g(A) \in \mathfrak{U}$. Tercero: $g(C) \subset A$. Entonces $g(C) \subset g(A)$ y, por lo tanto, $g(A) \in \mathfrak{U}$. La tercera condición sobre torres, o sea, que la unión de una cadena en $\mathfrak{U}$ pertenece a $\mathfrak{U}$, es inmediata a partir de la definición de $\mathfrak{U}$. Conclusión: $\mathfrak{U}$ es una torre incluida en $\mathfrak{J}_0$, y, por lo tanto, como $\mathfrak{J}_0$ es la torre más chica, $\mathfrak{U} = \mathfrak{J}_0$.

Las consideraciones precedentes implican que para cada conjunto comparable C el conjunto $g(C)$ es comparable también. Razón: dado C, fórmese $\mathfrak{U}$ como antes; el hecho de que $\mathfrak{U} = \mathfrak{J}_0$ significa que si $A \in \mathfrak{J}_0$, entonces $A \subset C$ (en cuyo caso $A \subset g(C)$) o bien $g(C) \subset A$.

Sabemos ahora que $\varnothing$ es comparable y que g transforma conjuntos comparables en conjuntos comparables. Como la unión de una cadena de conjuntos comparables es comparable, se sigue que los conjuntos comparables (de $\mathfrak{J}_0$) constituyen una torre y, por lo tanto, que agotan a $\mathfrak{J}_0$; esto es lo que señalamos para demostrar acerca de $\mathfrak{J}_0$.

Como $\mathfrak{J}_0$ es una cadena, la unión, digamos A, de todos los conjuntos de $\mathfrak{J}_0$ es ella misma un conjunto de $\mathfrak{J}_0$. Como la unión incluye a todos los conjuntos de $\mathfrak{J}_0$, se sigue que $g(A) \subset A$. Puesto que siempre $A \subset g(A)$, se sigue que $A = g(A)$, lo cual completa la demostración del lema de Zorn.

EJERCICIO. El lema de Zorn es equivalente al axioma de la elección. [Sugerencia para la demostración: dado un conjunto X, considérense las funciones f tales que dom $f \subset \mathcal{P}(X)$, ran $f \subset X$ y $f(A) \in A$ para todo A del dom f; ordénense estas funciones por extensión, úsese el lema de Zorn para encontrar una máxima entre ellas y demuestre que si f es máxima, entonces dom $f = \mathcal{P}(X) - \{\varnothing\}$]. Considérese cada una de las siguientes proposiciones y demuestre que también son equivalentes al axioma de la elección. (i) Todo conjunto parcialmente ordenado tiene una cadena máxima (a saber, una cadena que no es un subconjunto propio de ninguna otra cadena). (ii) Toda cadena de un conjunto parcialmente ordenado está incluida en alguna cadena máxima. (iii) Todo conjunto parcialmente ordenado en el cual cada cadena tenga una cota superior menor, tiene un elemento máximo.

SECCION 17

EL BUEN ORDEN

Un conjunto parcialmente ordenado puede no tener un primer elemento, y, aun teniéndolo, es perfectamente posible que alguno de sus subconjuntos no lo tenga. Se dice que un conjunto parcialmente ordenado está *bien ordenado* (y que su orden es un *buen orden*) si todos sus subconjuntos no vacíos tienen un primer elemento. Una consecuencia de esta definición que merece ser anotada aun antes de buscar ejemplos y contraejemplos, es que todo conjunto bien ordenado está totalmente ordenado. En realidad, si x y y son elementos de un conjunto bien ordenado, entonces $\{x, y\}$ es un subconjunto no vacío de ese conjunto bien ordenado y tiene, por lo tanto, un primer elemento; y según que ese elemento sea x o y, tendremos $x \leqq y$ o $y \leqq x$.

Para cada número natural n, el conjunto de todos los predecesores de n (o sea, de acuerdo con nuestras definiciones, el conjunto n) es un conjunto bien ordenado (ordenado por magnitud) y lo mismo es cierto para el conjunto ω de todos los números naturales. El conjunto $\omega \times \omega$, con $(a, b) \leqq (x, y)$ definido como $(2a + 1)2^y \leqq (2x + 1)2^b$ no está bien ordenado. Una manera de advertir esto es observando que $(a, b + 1) \leqq (a, b)$ para todo a y todo b, y se sigue que todo el conjunto $\omega \times \omega$ no tiene menor elemento.* Algunos subconjuntos de $\omega \times \omega$ sí tienen un menor elemento. Considérese, por ejemplo, el conjunto E de todas aquellas parejas (a, b) para las cuales $(1, 1) \leqq (a, b)$; el conjunto E tiene a $(1, 1)$ como su menor elemento. Advertencia: E, considerado como un conjunto parcialmente ordenado por su propio derecho, aún no está bien ordenado. El problema es que aun cuando E tenga un menor elemento, muchos subconjuntos de E no lo tienen; por ejemplo, considérese el conjun-

* Elemento menor o primero. Véanse las Págs. 86-87. (N. del R.)

to de todas aquellas parejas (a, b) de E para las cuales $(a, b) \neq (1, 1)$. Un ejemplo más: $\omega \times \omega$ está bien ordenado por su ordenamiento lexicográfico.

Uno de los hechos más gratos acerca del buen orden de los conjuntos, es que podemos demostrar cosas acerca de sus elementos por un proceso similar al de la inducción matemática. Concretamente, supóngase que S es un subconjunto de un conjunto bien ordenado X, y que siempre que un elemento x de X es tal que todo el segmento inicial $s(x)$ está incluido en S, entonces x mismo pertenece a S; el **principio de inducción transfinita** afirma que bajo estas circunstancias debemos tener $S = X$. Equivalentemente: si la presencia en un conjunto de todos los predecesores estrictos de un elemento implica siempre la presencia del elemento mismo, entonces el conjunto debe contener a todo.

Algunas observaciones resultan pertinentes antes de proceder con la demostración. El enunciado del principio ordinario de inducción matemática difiere del de la inducción transfinita en dos aspectos conspicuos. Uno: el último, en vez de pasar a cada elemento a partir de su predecesor, pasa a cada elemento a partir del conjunto de todos sus predecesores. Dos: en el último no hay ninguna suposición acerca de un elemento de partida (tal como el cero). La primera diferencia es importante: un elemento en un conjunto bien ordenado puede no tener un predecesor inmediato. Cuando este enunciado se aplica a ω puede demostrarse fácilmente que es equivalente al principio de inducción matemática; sin embargo, cuando este principio es aplicado a un conjunto bien ordenado arbitrario, no es equivalente al principio de inducción transfinita. Es decir: en general, los dos enunciados no son equivalentes entre sí; su equivalencia en ω es una circunstancia afortunada pero especial.

He aquí un ejemplo. Sea $X = \omega^+$, o sea, $X = \omega \cup \{\omega\}$ Defínase un orden en X ordenando los elementos de ω en la forma usual y requiriendo que $n < \omega$ para todo n de ω. El resultado es un conjunto bien ordenado. Pregunta: ¿Existe un subconjunto propio S de X tal que $0 \in S$ y que $n + 1 \in S$ siempre que $n \in S$? Respuesta: sí, a saber, $S = \omega$.

La segunda diferencia entre inducción ordinaria e inducción transfinita (no se necesita ningún elemento de partida para la segunda) es más linguística que conceptual. Si x_0 es el

elemento más chico de X, entonces $s(x_0)$ es vacío y, consecuentemente, $s(x_0) \subset S$; la hipótesis del principio de inducción transfinita requiere, por lo tanto, que x_0 pertenezca a S.

La demostración del principio de inducción transfinita es casi trivial. Si $X - S$ no es vacío, entonces tiene un elemento más chico, digamos x. Esto implica que todo elemento del segmento inicial $s(x)$ pertenece a S, y, por lo tanto, por la hipótesis de inducción, que x pertenece a S. Esto es una contradicción (x no puede pertenecer tanto a S como a $X - S$); la conclusión es que, después de todo, $X - S$ es vacío.

Diremos que un conjunto bien ordenado A es una *continuación* de un conjunto bien ordenado B si, en primer lugar, B es un subconjunto de A, si, de hecho, B es un segmento inicial de A y finalmente, si el ordenamiento de los elementos en B es el mismo que su ordenamiento en A. Luego, si X es un conjunto bien ordenado y si a y b son elementos de X con $b < a$, tendremos que $s(a)$ es una continuación de $s(b)$ y, por supuesto, que X es una continuación tanto de $s(a)$ como de $s(b)$.

Si $\mathcal{C}$ es una colección arbitraria de segmentos iniciales de un conjunto bien ordenado, entonces $\mathcal{C}$ es una cadena con respecto a la continuación, lo cual significa que $\mathcal{C}$ es una colección de conjuntos bien ordenados con la propiedad de que uno de dos miembros cualesquiera de la colección es una continuación del otro. Una forma de recíproco de este comentario es también cierto y frecuentemente útil. Si una colección $\mathcal{C}$ de conjuntos bien ordenados es una cadena con respecto a la continuación, y si U es la unión de los conjuntos de $\mathcal{C}$, entonces existe un buen orden único de U tal que U es una continuación de cada conjunto (distinto de U mismo) de la colección $\mathcal{C}$. Hablando toscamente, la unión de una cadena de conjuntos bien ordenados está bien ordenada. Esta formulación abreviada es peligrosa porque no aclara que la "cadena" es con respecto a la continuación. Si el ordenamiento implicado por la palabra "cadena" es tomado simplemente como una inclusión que preserva el orden, entonces la conclusión no es válida.

La demostración está ahora libre de obstáculos. Si a y b están en U, entonces existen conjuntos A y B en $\mathcal{C}$ con $a \in A$ y $b \in B$. Ya que o $A = B$, o bien, uno de entre A y B es una continuación del otro, se sigue que en cada caso tanto a como b

pertenecen a algún conjunto de $\mathcal{C}$; el orden de U está definido al ordenar cada pareja $\{a, b\}$ en la forma en que está ordenada en cada conjunto de $\mathcal{C}$ que contenga tanto a a como a b. Como $\mathcal{C}$ es una cadena, este orden está determinado sin ambigüedad. (Una forma alternativa de definir el orden prometido para U es la de recordar que los órdenes dados, en los conjuntos de $\mathcal{C}$, son conjuntos de parejas ordenadas, y formar la unión de todos esos conjuntos de parejas ordenadas).

Una verificación directa muestra que la relación definida en el párrafo precedente es en realidad un orden y que, más aún, su construcción nos fue obligada en cada paso (o sea, que el orden final está determinado unívocamente por los órdenes dados). La demostración de que el resultado es realmente un buen ordenamiento es igualmente directa. Cada subconjunto no vacío de U debe tener una intersección no vacía con algún conjunto de $\mathcal{C}$ y, por lo tanto, debe tener un primer elemento en ese conjunto; el hecho de que $\mathcal{C}$ es una cadena de continuación implica que ese primer elemento es necesariamente el primer elemento también de U.

> Ejercicio. Un subconjunto A de un conjunto parcialmente ordenado X es *cofinal* en X en caso de que para cada elemento x de X exista un elemento a de A tal que $x \leqq a$. Demuestre que todo conjunto totalmente ordenado tiene un subconjunto bien ordenado cofinal.

La importancia del buen ordenamiento emana del siguiente resultado, a partir del cual podemos inferir, entre otras cosas, que el principio de inducción transfinita es mucho más extensivamente aplicable de lo que podría indicar una mirada ocasional.

Teorema del buen ordenamiento. *Todo conjunto puede ser bien ordenado.*

Discusión. Un mejor enunciado (pero menos tradicional) es éste: para cada conjunto X, existe un buen ordenamiento con dominio X. Advertencia: no se ha dicho que el buen ordenamiento tenga relación alguna con cualquier otra estructura que el conjunto dado podría ya poseer. Si, por ejemplo, el lector sabe de algunos conjuntos parcial o totalmente ordenados cuyos ordenamientos no sean precisamente un buen ordenamiento, no debe saltar a la conclusión de que ha descubierto una paradoja. La única conclusión que puede inducirse es que algunos conjuntos pueden ser ordenados de muchas maneras, algunas de

las cuales son buenos ordenamientos y algunas otras no, y nosotros ya sabemos eso.

DEMOSTRACIÓN. Aplicamos el lema de Zorn. Dado el conjunto X, considérese la colección $\mathcal{W}$ de todos los subconjuntos bien ordenados de X. Explícitamente: un elemento de $\mathcal{W}$ es un subconjunto A de X junto con un buen ordenamiento de A. Ordenamos parcialmente a $\mathcal{W}$ por continuación.

La colección $\mathcal{W}$ no es vacía porque, por ejemplo, $\varnothing \in \mathcal{W}$. Si $X \neq \varnothing$, pueden exhibirse elementos más edificantes de $\mathcal{W}$, uno de ellos es $\{(x, x)\}$, para cualquier elemento particular x de X. Si $\mathcal{C}$ es una cadena en $\mathcal{W}$, entonces la unión U de los conjuntos de $\mathcal{C}$ tiene un buen ordenamiento único que hace a U "más grande" que (o igual a) cada conjunto de $\mathcal{C}$; esto es precisamente lo que ha verificado nuestra discusión precedente de la continuación. Esto significa que la hipótesis principal del lema de Zorn ha sido verificada; la conclusión es que existe un conjunto bien ordenado máximo, digamos M, en $\mathcal{W}$. El conjunto M debe ser igual a todo el conjunto X. Razón: si x es un elemento de X y no de M, M puede ser aumentado poniendo a x después de todos los elementos de M. La formulación rigurosa de esta descripción informal pero no ambigua se deja como un ejercicio para el lector. Con eso fuera del camino, la demostración del teorema del buen orden queda completa.

EJERCICIO. Demuestre que un conjunto totalmente ordenado está bien ordenado si y sólo si el conjunto de predecesores estrictos de cada elemento está bien ordenado. ¿Es aplicable alguna condición tal a conjuntos parcialmente ordenados? Demuestre que el teorema del buen orden implica el axioma de la elección (y por lo tanto, es equivalente a ese axioma y al lema de Zorn). Demuestre que si R es un orden parcial en un conjunto X, entonces existe un orden total en X, digamos S, tal que $R \subset S$; en otras palabras, cualquier orden parcial puede ser extendido a un orden total sin aumentar el dominio.

SECCION 18

INDUCCION TRANSFINITA

El proceso de "definición por inducción" tiene un análogo transfinito. El teorema ordinario de inducción construye una función en ω; la materia prima es una manera de obtener el valor de la función para cada elemento n distinto de cero de ω a partir de su valor para el elemento que precede a n. El análogo transfinito construye una función en cualquier conjunto ordenado W; la materia prima es una manera de obtener el valor de la función para cada elemento a de W a partir de sus valores para todos los predecesores de a.

Introduciremos algunos conceptos auxiliares con el fin de poder expresar el resultado en forma concisa. Si a es un elemento de un conjunto bien ordenado W, y X es un conjunto arbitrario, entonces por una *sucesión del tipo a en X* significaremos una función del segmento inicial de a en W hacia X. Las sucesiones del tipo a, para a en ω^+, son justamente a lo que hemos llamado sucesiones anteriormente, finitas o infinitas según que $a < \omega$ o $a = \omega$. Si U es una función de W a X, entonces la restricción de U al segmento inicial $s(a)$ de a es un ejemplo de una sucesión del tipo a para cada a en W; en lo subsecuente hallaremos conveniente denotar a esa sucesión por U^a [en vez de $U|s(a)$].

Una *función de sucesión del tipo W en X* es una función f cuyo dominio está constituido por todas las sucesiones del tipo a en X, para todos los elementos a de W y cuyo rango está incluido en X. Hablando toscamente, una función de sucesión nos dice cómo "alargar" una sucesión; dada una sucesión que llega hasta un elemento de W (sin incluirlo) pode-

mos usar una función de sucesión para añadirle un término más.

Teorema de inducción transfinita. *Si W es un conjunto bien ordenado y f una función de sucesión del tipo W en un conjunto X, entonces existe una función única U de W hacia X tal que $U(a) = f(U^a)$ para cada a de W.*

Demostración. La demostración del carácter único es una inducción transfinita sencilla. Para demostrar la existencia, se requiere que una función de W a X sea cierta clase de subconjunto de $W \times X$; construiremos U explícitamente como un conjunto de parejas ordenadas. Dígase que un subconjunto A de $W \times X$ *es f-cerrado* si tiene la siguiente propiedad: siempre que $a \in W$ y t sea una sucesión del tipo a incluida en A (esto es, $(c, t(c)) \in A$ para todo c del segmento inicial $s(a)$), entonces $(a, f(t)) \in A$. Como $W \times X$ mismo es f-cerrado, tales conjuntos existen; sea U la intersección de todos ellos. Como U mismo es f-cerrado, sólo resta demostrar que U es una función. En otras palabras, tenemos que demostrar que para cada c de W existe cuando mucho un elemento x de X tal que $(c, x) \in U$. (Explícitamente: si tanto (c, x) como (c, y) pertenecen a U, entonces $x = y$). La demostración es inductiva. Sea S el conjunto de todos aquellos elementos c de W para los cuales es en verdad cierto que $(c, x) \in U$ para un x cuando mucho. Demostraremos que si $s(a) \subset S$, entonces $a \in S$.

Decir que $s(a) \subset S$ significa que si $c < a$ en W, entonces existe un elemento único x en X tal que $(c, x) \in U$. La correspondencia $c \to x$ así definida es una sucesión del tipo a, digamos t, y $t \subset U$. Si a no pertenece a S, entonces $(a, y) \in U$ para algún y diferente de $f(t)$. Afirmación: el conjunto $U - \{(a, y)\}$ es f-cerrado. Esto significa que si $b \in W$ y si r es una sucesión del tipo b incluida en $U - \{(a, y)\}$, entonces $(b, f(r)) \in U - \{(a, y)\}$. De hecho, si $b = a$, entonces r debe ser t (por la afirmación de unicidad del teorema) y la razón por la cual el conjunto disminuido contiene a $(b, f(r))$ es que $f(t) \neq y$; si, en cambio, $b \neq a$, entonces la razón por la cual el conjunto disminuido contiene a $(b, f(r))$ es que U es f-cerrado (y, $b \neq a$). Esto contradice el hecho de que U es el conjunto f-cerrado más chico, y podemos concluir que $a \in S$.

Esto completa la demostración de la afirmación de existencia del teorema de la inducción transfinita. Una aplicación del mismo es llamada *definición por inducción transfinita*.

Continuaremos con una parte importante de la teoría del orden, la cual, incidentalmente, servirá también como una ilustración de cómo puede ser aplicado el teorema de la inducción transfinita.

Dos conjuntos parcialmente ordenados (los cuales pueden estar, en particular, totalmente ordenados y hasta bien ordenados) son llamados *semejantes* si existe entre ellos una correspondencia uno a uno que preserve el orden. Más explícitamente, decir que los conjuntos X y Y son semejantes (en símbolos $X \cong Y$) significa que existe una correspondencia uno a uno, digamos f, de X sobre Y, tal que si a y b están en X, entonces una condición necesaria y suficiente para que $f(a) \leqq f(b)$ (en Y) es que $a \leqq b$ (en X) Una correspondencia tal como f es a veces conocida como una *semejanza*.

EJERCICIO. Demuestre que la semejanza conserva a $<$ (en el mismo sentido en el que la definición exige la conservación de $\leqq$) y que, de hecho, una función uno a uno que transforma un conjunto parcialmente ordenado sobre otro es una semejanza si y sólo si preserva a $<$.

La transformación identidad en un conjunto parcialmente ordenado X es una semejanza de X sobre X. Si X y Y son conjuntos parcialmente ordenados y si f es una semejanza de X sobre Y, entonces (como f es uno a uno) existe una función inversa f^{-1}, bien determinada, de Y sobre X, y f^{-1} es una semejanza. Más aún, si g es una semejanza de Y sobre un conjunto parcialmente ordenado Z, entonces la composición gf es una semejanza de X sobre Z. De estas observaciones se sigue que, si restringimos nuestra atención a algún conjunto particular E y si, por lo tanto, consideramos sólo aquellos órdenes parciales cuyo dominio es un subconjunto de E, entonces la semejanza es una relación de equivalencia en el conjunto de conjuntos parcialmente ordenados así obtenido. Lo mismo sucede si limitamos el campo aún más y consideramos sólo los buenos ordenamientos cuyo dominio está incluido en E; la semejanza es una relación de equivalencia en el conjunto de conjuntos bien ordenados así obtenido. Aun cuando la semejanza fue definida para conjuntos parcialmente ordenados en completa generalidad, y el concepto puede ser estudiado en ese nivel, nuestro interés en lo

subsecuente se dirigirá solamente a la semejanza de conjuntos bien ordenados.

Es sobradamente posible que un conjunto bien ordenado sea semejante a un subconjunto propio; considérese como ejemplo, al conjunto de todos los números naturales y al conjunto de todos los números pares. (Como siempre, un número natural m es definido como par si existe un número natural n tal que $m = 2n$. La transformación $n \to 2n$ es una semejanza del conjunto de todos los números naturales sobre el conjunto de todos los números pares). Sin embargo, una semejanza entre un conjunto bien ordenado y una parte de él mismo es un tipo de transformación muy especial. De hecho, si f es una semejanza de un conjunto bien ordenado X en sí mismo, entonces $a \leqq f(a)$ para cada a de X. La demostración está basada directamente en la definición del buen orden. Si existen elementos b tales que $f(b) < b$, entonces existe uno menor entre ellos. Si $a < b$, siendo b ese menor, entonces $a \leqq f(a)$; en particular, se sigue, con $a = f(b)$, que $f(b) \leqq f(f(b))$. Sin embargo, ya que $f(b) < b$, el hecho de que f conserva el orden implica que $f(f(b)) < f(b)$. La única forma de eliminar la contradicción es admitiendo la imposibilidad de $f(b) < b$.

El resultado del párrafo precedente tiene tres consecuencias especialmente útiles. La primera de ellas es el hecho de que si dos conjuntos bien ordenados, X y Y digamos, son de alguna manera semejantes, entonces hay justamente una semejanza entre ellos. En efecto, supóngase que tanto g como h son semejanzas de X sobre Y y escriba $f = g^{-1}h$. Como f es una semejanza de X sobre sí mismo, se sigue que $a \leqq f(a)$ para cada a de X. Esto significa que $a \leqq g^{-1}(h(a))$ para cada a de X. Aplicando g, inferimos que $g(a) \leqq h(a)$ para cada a de X. La situación es simétrica en g y h, de manera que podemos inferir también que $h(a) \leqq g(a)$ para cada a de X. Conclusión: $g = h$.

Una segunda consecuencia es el hecho de que un conjunto bien ordenado nunca es semejante a uno de sus segmentos iniciales. En efecto, si X es un conjunto bien ordenado, a un elemento de X y f una semejanza de X sobre $s(a)$, entonces, en particular, $f(a) \in s(a)$, de manera que $f(a) < a$, lo cual es imposible.

La tercera y principal consecuencia es el teorema de la comparabilidad para conjuntos bien ordenados. Lo que se afirma es que si X y Y son conjuntos bien ordenados, entonces o

X y Y son semejantes o bien uno de ellos es semejante a un segmento inicial del otro. Sólo como práctica usaremos el teorema de la inducción transfinita en la demostración, pues es muy fácil eludirlo si se desea. Suponemos que X y Y son conjuntos bien ordenados no vacíos tales que ninguno es semejante a un segmento inicial del otro, y procederemos a demostrar que bajo estas circunstancias X debe ser semejante a Y. Supóngase que $a \in X$ y que t es una sucesión del tipo a en Y; en otras palabras, t es una función de $s(a)$ hacia Y. Sea $f(t)$ la menor de las cotas superiores propias del rango de t en Y, si es que hay alguna; y, si no la hay, permítase que $f(t)$ sea el menor elemento de Y. En la terminología del teorema de la inducción transfinita, la función f así determinada es una función de sucesión del tipo X en Y. Sea U la función que el teorema de inducción transfinita asocia a esta situación. Un razonamiento sencillo (por inducción transfinita) muestra que, para cada z en X la función U transforma en forma uno a uno al segmento inicial determinado por a en X sobre el segmento inicial determinado por $U(a)$ en Y. Esto implica que U es una semejanza, lo cual completa la demostración.

He aquí un bosquejo de una demostración alternativa que no se sirve del teorema de inducción transfinita. Sea X_0 el conjunto de todos aquellos elementos a de X para los cuales existe un elemento b de Y tal que $s(a)$ es semejante a $s(b)$. Para cada a de X_0, escriba $U(a)$ para el correspondiente (determinado en forma única) b de Y, y sea Y_0 el rango de U. Se sigue que $X_0 = X$, o bien, que X_0 es un segmento inicial de X y $Y_0 = Y$.

EJERCICIO. Cada subconjunto de un conjunto bien ordenado X es semejante a X o a un segmento inicial de X. Si X y Y son conjuntos bien ordenados y $X \cong Y$ (esto es, que X es semejante a Y), entonces la semejanza transforma a la menor cota superior (si hay alguna) de cada subconjunto de X sobre la menor cota superior de la imagen de tal subconjunto.

SECCION 19

NUMEROS ORDINALES

El sucesor x^+ de un conjunto x fue definido como $x \cup \{x\}$, y entonces ω fue construido como el conjunto más chico que contiene a 0 y que contiene a x^+ siempre que contiene a x. ¿Qué sucede si comenzamos con ω, formamos su sucesor ω^+, después el sucesor de éste y continuamos así ad infinitum? En otras palabras, ¿hay algo más allá de ω, ω^+, $(\omega^+)^+$, . . . , etc., en el mismo sentido en el que ω está más allá de, 0 1, 2, . . . , etc.?

La pregunta reclama un conjunto, digamos T, que contenga a ω, tal que cada elemento de T (distinto de ω mismo) pueda ser obtenido a partir de ω mediante la formación repetida de sucesores. Para formular más precisamente este requerimiento introduciremos alguna terminología especial provisional. Digamos que una función f cuyo dominio es el conjunto de todos los predecesores estrictos de algún número natural n (en otras palabras, dom $f = n$) es una *función a los sucesores de* ω* si $f(0) = \omega$ (siempre que $n \neq 0$, de manera que $0 < n$) y $f(m^+) = (f(m))^+$ siempre que $m^+ < n$. Una demostración sencilla por inducción matemática muestra que para cada número natural n existe una única función a los sucesores de ω con dominio n. Decir que algo o es igual a ω o puede ser obtenido de ω mediante la formación repetida de sucesores, significa que pertenece al rango de alguna función a los sucesores de ω. Sea $S(n, x)$ la frase que dice "n es un número natural y x pertenece al rango de la función a los sucesores con dominio n". Un conjunto T tal que $x \in T$ si, y sólo si, $S(n, x)$ es verdadera para algún n es lo que andamos buscando; tal conjunto está tan alejado de ω como ω lo está de 0.

Sabemos que para cada número natural n nos está permitido formar el conjunto $\{x : S(n, x)\}$. En otras palabras, para cada número natural n, existe un conjunto $F(n)$ tal que $x \in F(n)$ si y sólo si $S(n, x)$ es verdadera. La conexión entre n y $F(n)$ parece, en mucho, ser algo como una función. Sin embargo, sucede que ninguno de los métodos para la construcción de conjuntos que hemos visto hasta el momento es lo suficientemente fuerte para demostrar la existencia de un conjunto F de parejas ordenadas tal que $(n, x) \in F$ si, y sólo si $x \in F(n)$. Para lograr este obviamente deseable estado de cosas, necesitamos un principio más en la teoría de los conjuntos (que será el último). Hablando toscamente, el nuevo principio dice que cualquier cosa sensata que pueda uno hacer a los elementos de un conjunto produce un conjunto.

Axioma de la sustitución. *Si $S(a, b)$, es una frase tal que para cada a de un conjunto A el conjunto $\{b : S(a, b)\}$ puede ser formado, entonces existe una función F con dominio A tal que $F(a) = \{b : S(a, b)\}$ para cada a de A.*

Decir que $\{b : S(a, b)\}$ puede ser formado significa, por supuesto, que existe un conjunto $F(a)$ tal que $b \in F(a)$ si y sólo si $S(a, b)$ es verdadera. El axioma de la extensión implica que la función descrita en el axioma de la sustitución está determinada unívocamente por la frase dada y el conjunto dado. La razón para el nombre del axioma es que nos permite formar un nuevo conjunto a partir de uno original sustituyendo a cada elemento de éste por algo nuevo.

La principal aplicación del axioma de la sustitución consiste en extender el proceso de contar más allá de los números naturales. Desde el punto de vista actual, la propiedad crucial de un número natural es que es un conjunto bien ordenado tal que el segmento inicial determinado por cada elemento es igual a ese elemento. (Recuérdese que si m y n son números naturales, entonces $m < n$ significa $m \in n$, y esto implica que $\{m \in \omega : m < n\} = n$). Esta es la propiedad sobre la cual está basado el proceso de contar extendido; la definición fundamental en este círculo de ideas se debe a von Neumann. Un *número ordinal* está definido como un conjunto bien ordenado α tal que $s(\xi) = \xi$ para todo ξ de α; $s(\xi)$ es aquí, como antes, el segmento inicial $\{\eta \in \alpha : \eta < \xi\}$.

Un ejemplo de un número ordinal que no es un número natural es el del conjunto ω constituido por todos los números naturales. Esto significa que ya podemos "contar" más allá de lo que podíamos antes; mientras que antes los únicos números a nuestra disposición eran los elementos de ω, ahora tenemos a ω mismo. También tenemos al sucesor ω^+ de ω; este conjunto está ordenado en la manera obvia y, más aún, el ordenamiento obvio es un buen ordenamiento que satisface la condición impuesta a los números ordinales. En realidad, si $\xi \in \omega^+$, entonces, por la definición de sucesor, se tiene $\xi \in \omega$, en cuyo caso sabemos ya que $s(\xi) = \xi$, o bien $\xi = \omega$, en cuyo caso, por la definición de orden, $s(\xi) = \omega$, de manera que, nuevamente, $s(\xi) = \xi$. El razonamiento acabado de presentar es completamente general y demuestra que si α es un número ordinal, entonces también lo es α^+. Se sigue que nuestro proceso de contar se extiende ahora hasta e incluyendo ω, y ω^+, y $(\omega^+)^+$, y así sucesivamente al infinito.

En este punto hacemos contacto con nuestro estudio anterior de lo que sucede más allá de ω. El axioma de la sustitución implica que existe una función única F definida en ω tal que $F(0) = \omega$ y $F(n^+) = [F(n)]^+$ para cada número natural n. El rango de esta función es un conjunto de interés para nosotros, y de más importancia aún es el conjunto consistente en la unión del conjunto ω con el rango de la función F. Por razones que se aclararán solamente hasta que hayamos dado cuando menos una ojeada a la aritmética de los números ordinales, dicha unión se denota usualmente por $\omega 2$. Si, anticipando otra vez la notación de la aritmética ordinal, escribimos $\omega + n$ por $F(n)$, entonces podemos describir al conjunto $\omega 2$ como el conjunto constituido por todos los n (con n en ω) y todos los $\omega + n$ (con n en ω).

Ahora es fácil verificar que $\omega 2$ es un número ordinal. La verificación depende, por supuesto, de la definición de orden en $\omega 2$. En este momento tanto esta definición como la demostración son dejadas como ejercicios; nuestra atención oficial se enfoca hacia algunas observaciones generales que incluyen los hechos acerca de $\omega 2$ como casos especiales sencillos.

Un orden (parcial o total) en un conjunto X está en forma única determinado por sus segmentos iniciales. En otras palabras, si R y S son órdenes en X, y si para cada x de X, el conjunto de todos los predecesores-R de x es el mismo que el conjunto

de todos los predecesores-S de x, entonces R es lo mismo que S. Esta afirmación es obvia independientemente de que los predecesores se tomen en sentido estricto o no. La afirmación se aplica, en particular, a conjuntos bien ordenados. A partir de este caso especial inferimos, que si acaso es posible bien ordenar un conjunto a modo de convertirlo en un número ordinal, entonces sólo hay una manera de hacerlo. El conjunto por sí solo nos dice cuál debe ser la relación que hace de él un número ordinal; si dicha relación satisface los requerimientos, entonces el conjunto es un número ordinal, y de otra manera no lo es. Decir que $s(\xi) = \xi$ significa que los predecesores de ξ deben ser justamente los elementos de ξ. La relación en cuestión es, por lo tanto, simplemente la relación de pertenencia. Si $\eta < \xi$ es definida como $\eta \in \xi$ siempre que ξ y η son elementos de un conjunto α, entonces el resultado puede ser o no un buen ordenamiento de α tal que $s(\xi) = \xi$ para cada ξ en α, y α es un número ordinal en el primer caso y no en el otro.

Concluiremos con este estudio preliminar de los números ordinales mencionando los nombres de algunos de los primeros de ellos. Después de 0, 1, 2, ... viene ω, y después de ω, $\omega + 1$, $\omega + 2$, ... viene $\omega 2$. Después de $\omega 2 + 1$ (o sea, del sucesor de $\omega 2$) viene $\omega 2 + 2$ y después $\omega 2 + 3$; en seguida, después de todos los términos de la sucesión así iniciada, viene $\omega 3$. (Aquí se hace necesaria otra aplicación del axioma de la sustitución). En seguida viene $\omega 3 + 1$, $\omega 3 + 2$, $\omega 3 + 3$, ..., y después de ellos viene $\omega 4$. En esta forma obtenemos sucesivamente ω, $\omega 2$, $\omega 3$, $\omega 4$, ... Una aplicación del axioma de la sustitución conduce a algo que les sigue a todos ellos en el mismo sentido en que ω sigue a los números naturales; ese algo es ω^2. Después de esto todo el proceso se inicia nuevamente: $\omega^2 + 1$, $\omega^2 + 2$, ..., $\omega^2 + \omega$, $\omega^2 + \omega + 1$, $\omega^2 + \omega + 2$, ..., $\omega^2 + \omega 2$, $\omega^2 + \omega 2 + 1$, ..., $\omega^2 + \omega 3$, ..., $\omega^2 + \omega 4$, ..., $\omega^2 2$, ..., $\omega^2 3$, ..., ω^3, ..., ω^4, ..., ω^ω, ..., $\omega^{(\omega^\omega)}$, ..., $\omega^{(\omega^{(\omega^\omega)})}$, ... El que sigue a todo esto es ε_0; después viene $\varepsilon_0 + 1$, $\varepsilon_0 + 2$, ..., $\varepsilon_0 + \omega$, ..., $\varepsilon_0 + \omega 2$, ..., $\varepsilon_0 + \omega^2$, ..., $\varepsilon_0 + \omega^\omega$, ..., $\varepsilon_0 2$, ..., $\varepsilon_0 \omega$, ..., $\varepsilon_0 \omega^\omega$, ..., ε_0^2, ...

SECCION 20

CONJUNTOS DE NUMEROS ORDINALES

Un número ordinal es, por definición, un género especial de conjunto bien ordenado; procederemos a examinar sus propiedades especiales.

El hecho más elemental es que cada elemento de un número ordinal α es a la vez un subconjunto de α. (En otras palabras, todo número ordinal es un conjunto transitivo). En realidad, si $\xi \in \alpha$, entonces el hecho de que $s(\xi) = \xi$ implica que cada elemento de ξ es un predecesor de ξ en α y por consiguiente, en particular, un elemento de α.

Si ξ es un elemento de un número ordinal α, entonces, como acabamos de ver, ξ es un subconjunto de α y, consecuentemente, ξ es un conjunto bien ordenado (con respecto al ordenamiento que hereda de α). Afirmación: ξ es de hecho un número ordinal. En efecto, si $\eta \in \xi$, entonces el segmento inicial determinado por η en ξ es el mismo que el segmento inicial determinado por η en α; como el último es igual a η, también lo es el primero. Otra manera de formular el mismo resultado es diciendo que todo segmento inicial de un número ordinal es un número ordinal.

El siguiente hecho a anotar es que si dos números ordinales son semejantes, entonces son iguales. Para demostrarlo, supóngase que α y β son números ordinales y que f es una semejanza de α sobre β; debemos hacer ver que $f(\xi) = \xi$ para cada ξ de α. La demostración es una inducción transfinita directa. Escríbase $S = \{\xi \in \alpha : f(\xi) = \xi\}$. Para cada ξ de α, el menor elemento de α que no pertenece a $s(\xi)$ es ξ mismo. Como f es una semejanza se sigue que el menor elemento de β que no pertenece a la imagen de $s(\xi)$ bajo f es $f(\xi)$. Estos asertos implican que si $s(\xi) \subset S$, entonces $f(\xi)$ y ξ son números ordinales con los mis-

mos segmentos iniciales, y, por consiguente, que $f(\xi) = \xi$. Hemos demostrado entonces que $\xi \in S$ siempre que $s(\xi) \subset S$. El principio de inducción transfinita implica que $S = \alpha$, y de esto se sigue que $\alpha = \beta$.

Si α y β son números ordinales, entonces, en particular, son conjuntos bien ordenados, y, consecuentemente, o son semejantes o, bien, uno de ellos es semejante a un segmento inicial del otro. Si, digamos, β es semejante a un segmento inicial de α, entonces β es semejante a un elemento de α. Como todo elemento de α es un número ordinal, se sigue que β *es* un elemento de α o, aún en otras palabras, que α es una continuación de β. Sabemos por ahora que si α y β son números ordinales diferentes entre sí, entonces las proposiciones

$$\beta \in \alpha,$$

$$\beta \subset \alpha.$$

α *es una continuación de* β,

son equivalentes entre sí y, si se cumplen, podemos escribir

$$\beta < \alpha$$

Lo que acabamos de demostrar es que dos números ordinales cualesquiera son comparables; o sea, que si α y β son números ordinales, entonces $\beta = \alpha$ o $\beta < \alpha$ o $\alpha < \beta$.

El resultado del párrafo precedente puede ser expresado diciendo que todo conjunto de números ordinales está totalmente ordenado. En realidad hay más: todo conjunto de números ordinales está bien ordenado. En efecto, supóngase que E es un conjunto no vacío de números ordinales y permítase que α sea un elemento de E. Si $\alpha \leqq \beta$ para todo β en E, entonces α es el primer elemento de E y todo está bien. Si no es este el caso, entonces existe un elemento β en E tal que $\beta < \alpha$, o sea, que $\beta \in \alpha$; en otras palabras, entonces $\alpha \cap E$ no es vacío. Como α es un conjunto bien ordenado, $\alpha \cap E$ tiene un primer elemento, digamos α_0. Si $\beta \in E$, entonces o $\alpha \leqq \beta$ (en cuyo caso $\alpha_0 < \beta$), o bien $\beta < \alpha$ (en cuyo caso $\beta \in \alpha \cap E$ y, por lo tanto, $\alpha_0 \leqq \beta$), y esto demuestra que E tiene un primer elemento, a saber, α_0.

Algunos números ordinales son finitos; ellos son precisamente los números naturales (o sea, los elementos de ω). Los demás son llamados *transfinitos* y el conjunto ω de todos los números naturales es el número ordinal transfinito más pequeño.

Cada número ordinal finito (distinto de 0) tiene un predecesor inmediato. Si un número ordinal transfinito α tiene un predecesor inmediato β, entonces, tal como sucede con los números naturales, $\alpha = \beta^+$. No todo número ordinal transfinito tiene un predecesor inmediato; aquellos que no lo tienen son llamados *números límite*.

Supóngase ahora que $\mathcal{C}$ es una colección de números ordinales. Ya que, como acabamos de ver, $\mathcal{C}$ es una cadena por continuación, se sigue que la unión α de los conjuntos de $\mathcal{C}$ es un conjunto bien ordenado tal que para todo ξ de $\mathcal{C}$, distinto de α mismo, α es una continuación de ξ. El segmento inicial determinado por un elemento de α es el mismo que el segmento inicial determinado por ese elemento cualquiera que sea el conjunto de $\mathcal{C}$ en que se presente; esto implica que α es un número ordinal. Si $\xi \in \mathcal{C}$, entonces $\xi \leqq \alpha$ y el número α es una cota superior de los elementos de $\mathcal{C}$. Si β es otra cota superior de $\mathcal{C}$, entonces $\xi \subset \beta$ siempre que $\xi \in \mathcal{C}$, y, por lo tanto, por la definición de las uniones, $\alpha \subset \beta$. Esto implica que α es la menor cota superior de $\mathcal{C}$ y hemos demostrado así que todo conjunto de números ordinales tiene un supremo.

¿Hay algún conjunto constituido precisamente por todos los números ordinales? Es fácil ver que la respuesta debe ser no. Si existiera conjunto tal, podríamos formar el supremo de todos los números ordinales. Tal supremo sería un número ordinal mayor o igual que cada número ordinal. Sin embargo, esto es imposible, ya que para cada número ordinal existe uno estrictamente mayor (por ejemplo, su sucesor) y, así, no tiene sentido hablar del "conjunto" de todos los ordinales. La contradicción, basada en la suposición de que tal conjunto existe, es conocida como la *paradoja de Burali-Forti.* (Burali-Forti fue una persona, no dos).

Nuestro siguiente propósito es el de hacer ver que el concepto del número ordinal no es tan especial como podría parecer y que, en realidad, cada conjunto bien ordenado se asemeja a un número ordinal en todos los aspectos esenciales. La "semejanza" es mencionada aquí con el sentido técnico de la palabra. Un enunciado informal del resultado es que cada conjunto bien ordenado puede ser contado.

Teorema del conteo. *Cada conjunto bien ordenado es semejante a un número ordinal único.*

DEMOSTRACION. Ya que para los números ordinales la semejanza es lo mismo que la igualdad, el carácter de unicidad es obvio. Supóngase ahora que X es un conjunto bien ordenado y que un elemento a de X es tal que el segmento inicial determinado por cada predecesor de a es semejante a algún número ordinal (necesariamente único). Si $S(x, \alpha)$ es la frase que dice "α es un número ordinal y $s(x) \cong \alpha$", entonces, para cada x en $s(a)$, el conjunto $\{\alpha : S(x, \alpha)\}$ puede ser formado; de hecho, tal conjunto es un conjunto singular. El axioma de la sustitución implica la existencia de un conjunto constituido precisamente por los números ordinales semejantes a los segmentos iniciales determinados por los predecesores de a. Independientemente de que a sea el sucesor inmediato de uno de sus predecesores o el supremo de todos ellos, se sigue que $s(a)$ es semejante a un número ordinal. Este razonamiento prepara el camino para una aplicación del principio de inducción transfinita y la conclusión es que cada segmento inicial en X es semejante a algún número ordinal. Este hecho, a su vez, justifica otra aplicación del axioma de la sustitución, tal como la que se hizo anteriormente; la conclusión final es, como se deseaba, que X es semejante a algún número ordinal.

SECCION 21

ARITMETICA ORDINAL

En los números naturales hemos usado el teorema de la inducción para definir las operaciones aritméticas y, subsecuentemente, hemos demostrado que esas operaciones están relacionadas con las operaciones de la teoría de los conjuntos en varias maneras convenientes. Así, por ejemplo, sabemos que el número de elementos de la unión de dos conjuntos finitos ajenos E y F es igual a $\#(E) + \#(F)$. Ahora advertimos que este hecho pudo haber sido empleado para definir la adición. Si m y n son números naturales, pudimos haber definido su suma encontrando conjuntos ajenos E y F, con $\#(E) = m$ y $\#(F) = n$, y escribiendo $m + n = \#(E \cup F)$.

Correspondiendo a lo que se hizo y a lo que pudo haber sido hecho en los números naturales, hay dos vías de entrada típicas a la aritmética ordinal. Parte por variar y parte porque en este contexto la inducción parece menos natural, enfatizaremos la introducción con base en la teoría de conjuntos en vez de la basada en la inducción.

Comenzaremos por indicar que hay una manera más o menos obvia de reunir dos conjuntos bien ordenados para formar un nuevo conjunto bien ordenado. Hablando informalmente, la idea es escribir uno de ellos y seguirlo entonces por el otro. Si tratamos de decir esto rigurosamente, encontramos inmediatamente la dificultad de que los conjuntos pueden no ser ajenos. ¿Cuándo se supone que escribamos un elemento que es común a los dos conjuntos? La manera de salir de la dificultad es haciéndolos ajenos. Esto puede lograrse pintando a sus elementos de distintos colores. En un lenguaje más matemático, reemplácense los elementos de los conjuntos por

esos mismos elementos tomados junto con un objeto distintivo, empleando una etiqueta para cada conjunto. En lenguaje completamente matemático: si E y F son dos conjuntos arbitrarios, sea $\hat{E}$ el conjunto de todas las parejas ordenadas $(x, 0)$ con x en E, y sea $\hat{F}$ el conjunto de todas las parejas ordenadas $(x, 1)$ con x en F. Es claro que los conjuntos $\hat{E}$ y $\hat{F}$ son ajenos entre sí. Entre los conjuntos E y $\hat{E}$ hay una correspondencia uno a uno obvia $[x \rightarrow (x, 0)]$, y otra entre F y $\hat{F}$ $[x \rightarrow (x, 1)]$ Estas correspondencias pueden ser usadas para trasladar a $\hat{E}$ y $\hat{F}$ cualquier estructura que puedan poseer E y F (por ejemplo, orden). Se sigue que siempre que nos sean dados dos conjuntos, con o sin alguna estructura adicional, podemos reemplazarlos por dos conjuntos ajenos con la misma estructura, por lo cual podemos suponer, sin pérdida de generalidad, que eran ajenos desde el principio.

Antes de aplicar esta construcción a la aritmética ordinal, advertimos que puede ser generalizada a familias arbitrarias de conjuntos. En efecto, si $\{E_i\}$ es una familia, escríbase $\hat{E}_i$ para el conjunto de todas las parejas ordenadas (x, i), con x en E_i. (En otras palabras, $\hat{E}_i = E_i \times \{i\}$). La familia $\{\hat{E}_i\}$ está constituida por conjuntos ajenos entre sí y puede hacer cualquier cosa que la familia original $\{E_i\}$ pueda hacer.

Supóngase ahora que E y F son conjuntos ajenos bien ordenados. Defínase el orden en $E \cup F$, de manera que las parejas de elementos en E, así como las parejas de elementos en F conserven el orden que tenían, y de manera que cada elemento de E preceda a cada elemento de F. [En lenguaje ultraformal: si R y S son las relaciones de orden dadas en E y F respectivamente, ordénese a $E \cup F$ por $R \cup S \cup (E \times F)$]. El hecho de que E y F estaban bien ordenados implica que $E \cup F$ esté bien ordenado. El conjunto bien ordenado $E \cup F$ es llamado *suma ordinal* de los conjuntos bien ordenados E y F.

Hay una manera sencilla y valiosa de extender el concepto de suma ordinal a un número infinito de sumandos. Supóngase que $\{E_i\}$ es una familia de conjuntos ajenos bien ordenados indicada por un conjunto bien ordenado I. La suma ordinal de la familia es la unión $\bigcup_i E_i$, ordenada en la forma siguiente. Si a y b son dos elementos de la unión, con $a \in E_i$ y $b \in E_j$, entonces $a < b$ significa que $i < j$, o bien, que $i = j$ y a precede a b en el orden dado en E_i.

La definición de adición para números ordinales es ahora un juego de niños. Para cada conjunto bien ordenado X, sea ord X el único número ordinal semejante a X. (Si X es finito entonces ord X es lo mismo que el número natural $\#(X)$ definido anteriormente). Si α y β son números ordinales, sean A y B dos conjuntos ajenos bien ordenados con ord $A = \alpha$ y ord $B = \beta$, y sea C la suma ordinal de A y B. La *suma* $\alpha + \beta$ es, por definición, el número ordinal de C, de manera que ord A + ord B = ord C. Es importante advertir que la suma $\alpha + \beta$ es independiente de la elección particular de los conjuntos A y B, ya que cualquier otro par de conjuntos ajenos con tales números ordinales, habría dado el mismo resultado.

Estas consideraciones se extienden sin dificultad al caso infinito. Si $\{\alpha_i\}$ es una familia bien ordenada de números ordinales indicados por un conjunto bien ordenado I, sea $\{A_i\}$ una familia de conjuntos ajenos bien ordenados con ord $A_i = \alpha_i$ para cada i y sea A la suma ordinal de la familia $\{A_i\}$. La suma $\sum_{i \in I}$ ord A_i es, por definición, el número ordinal de A, de manera que $\sum_{i \in I}$ ord A_i = ord A. También aquí el resultado es independiente de la elección arbitraria de los conjuntos bien ordenados A_i; cualesquiera otras elecciones (con los mismos números ordinales) habría dado la misma suma.

Algunas de las propiedades de la adición de números ordinales son buenas y otras son malas. Por el lado bueno están las identidades

$$\alpha + 0 = \alpha,$$
$$0 + \alpha = \alpha,$$
$$\alpha + 1 = \alpha^+,$$

y la ley asociativa

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma.$$

Igualmente loable es el hecho de que $\alpha < \beta$ si y sólo si existe un número ordinal γ distinto de 0 tal que $\beta = \alpha + \gamma$. Las demostraciones de todas estas proposiciones son elementales.

Casi todo el comportamiento desagradable de la adición emana de la falla de la ley conmutativa. Ejemplo: $1 + \omega = \omega$ (pero, como acabamos de ver, $\omega + 1 \neq \omega$). El mal comporta-

miento de la adición pone de manifiesto algunos hechos intuitivamente claros acerca del orden. Si, por ejemplo, anexamos un nuevo elemento al principio de una sucesión infinita (del tipo ω), el resultado es claramente semejante a aquello con lo cual empezamos, pero si, en cambio, lo anexamos al final, habremos arruinado la semejanza, ya que el conjunto original no tenía un último elemento y el nuevo sí lo tiene.

El uso principal de las sumas infinitas es el de motivar y facilitar el estudio de los productos. Si A y B son dos conjuntos bien ordenados, es natural definir su producto como el resultado de sumar A consigo mismo B veces. Para hacer que esto tenga sentido, debemos procurarnos antes que nada una familia de conjuntos ajenos bien ordenados, cada uno de los cuales es semejante a A, indicados por el conjunto B. La regla general para hacer esto funciona bien aquí, ya que todo lo que necesitamos hacer es escribir $A_b = A \times \{b\}$ para cada b de B. Si examinamos ahora la definición de suma ordinal como se aplica a la familia $\{A_b\}$, seremos llevados a formular la siguiente definición. El *producto ordinal* de dos conjuntos bien ordenados A y B es el producto cartesiano $A \times B$ con el orden lexicográfico inverso. En otras palabras, si (a, b) y (c, d) están en $A \times B$, entonces $(a, b) < (c, d)$ significa que $b < d$ o bien, que $b = d$ y $a < c$.

Si α y β son números ordinales, sean A y B dos conjuntos bien ordenados con ord $A = \alpha$ y ord $B = \beta$, y sea C el producto ordinal de A y B. El *producto* $\alpha\beta$ es, por definición el número ordinal de C, de manera que (ord A) (ord B) = ord C. El producto está definido sin ambigüedades, independientemente de la elección arbitraria de los conjuntos bien ordenados A y B. Alternativamente, pudimos haber eliminado toda arbitrariedad en este punto recordando que el conjunto bien ordenado más a la mano que hay cuyo número ordinal es α, es el número ordinal α mismo (y análogamente para β).

Como la adición, la multiplicación tiene sus buenas y sus malas propiedades. Entre las buenas están las identidades

$$\alpha 0 = 0,$$

$$0\alpha = 0,$$

$$\alpha 1 = \alpha,$$

$$1\alpha = \alpha,$$

la ley asociativa

$$\alpha(\beta\gamma) = (\alpha\beta)\gamma,$$

la ley distributiva izquierda

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma,$$

y el hecho de que si el producto de dos números ordinales es cero, entonces uno de los factores debe ser cero. (Nótese que hemos usado la convención usual referente a que la multiplicación tiene lugar antes que la adición, o sea, que $\alpha\beta + \alpha\gamma$ significa $(\alpha\beta) + (\alpha\gamma)$).

La ley conmutativa de la multiplicación falla, así como también muchas de sus consecuencias. Así, por ejemplo, $2\omega = \omega$ (piense en una sucesión infinita de parejas ordenadas), pero $\omega 2 \neq \omega$ (piense en una pareja ordenada de sucesiones infinitas). La ley distributiva derecha también falla; o sea, que $(\alpha + \beta)\gamma$ es, en general, diferente de $\alpha\gamma + \beta\gamma$. Ejemplo: $(1 + 1)\omega = 2\omega = \omega$, mientras que $1\omega + 1\omega = \omega + \omega = \omega 2$.

Tal como la adición repetida condujo a la definición de productos ordinales, la multiplicación repetida puede ser usada para definir exponentes ordinales. Alternativamente, puede llegarse a los exponentes por medio de la inducción transfinita. Los detalles precisos son parte de una extensa y altamente especializada teoría de números ordinales. Al respecto nos conformaremos con sugerir la definición y mencionar sus consecuencias más sencillas. Para definir α^β (donde α y β son números ordinales) úsese una definición por inducción transfinita (sobre β). Comiéncese escribiendo $\alpha^0 = 1$ y $\alpha^{\beta+1} = \alpha^\beta\alpha$; si β es un número límite, defínase α^β como el supremo de los números de la forma α^γ, donde $\gamma < \beta$. Si este bosquejo de definición es formulado con cuidado, se sigue que

$$0^\alpha = 0 \ (\alpha \geqq 1),$$

$$1^\gamma = 1,$$

$$\alpha^{\beta+\gamma} = \alpha^\beta\alpha^\gamma,$$

$$\alpha^{\beta\gamma} = (\alpha^\beta)^\gamma.$$

No se cumplen todas las leyes usuales para exponentes; así, por ejemplo, $(\alpha\beta)^\gamma$ generalmente no es lo mismo que $\alpha^\gamma\beta^\gamma$. Ejemplo: $(2 \cdot 2)^\omega = 4^\omega = \omega$, pero $2^\omega \cdot 2^\omega = \omega \cdot \omega = \omega^2$.

Advertencia: la notación exponencial para números ordinales, aquí y en adelante, no es consistente con nuestro primer uso

de los exponentes. El conjunto no ordenado 2^ω de todas las funciones de ω a 2, y el conjunto bien ordenado 2^ω que es la menor cota superior de la sucesión de números ordinales 2,2 · 2, 2 · 2 · 2, etc., no son la misma cosa en absoluto. No hay manera de evitarlo; la costumbre matemática está firmemente establecida en ambas partes. Si, en una situación particular el contexto no revela cuál de las dos interpretaciones debe tomarse, será necesario dar una indicación verbal explícita.

SECCION 22

EL TEOREMA DE SCHRÖDER-BERNSTEIN

El propósito de contar es el de comparar el tamaño de un conjunto con el de otro; el método más familiar de contar los elementos de un conjunto es el de arreglarlos en un orden apropiado. La teoría de los números ordinales es una ingeniosa abstracción del método, pero se queda un tanto corta en la realización del propósito. Esto no es decir que los números ordinales son inútiles; simplemente sucede que su aplicación principal está en otra parte, por ejemplo, en topología, como fuente de ejemplos y contraejemplos. En adelante, seguiremos prestando cierta atención a los números ordinales, pero dejarán de ocupar el centro de la escena. (Es de cierta importancia saber que, de hecho, podríamos prescindir totalmente de ellos. La teoría de los números cardinales puede ser construida con la ayuda de los números ordinales, o sin ella; ambos tipos de construcción tienen ventajas.) Con estas observaciones preliminares fuera del camino podemos pasar al problema de comparar los tamaños de los conjuntos.

El problema es el de comparar los tamaños de los conjuntos cuando sus elementos no parecen tener nada que ver unos con otros. Es bastante fácil decidir que hay más gente en Francia que en París. Sin embargo, no es tan fácil comparar la edad del universo en segundos con la población de París en electrones. Como algunos ejemplos de carácter matemático, considérense las siguientes parejas de conjuntos, definidas en términos de un conjunto auxiliar A: (i) $X = A$, $Y = A^+$; (ii) $X = \wp(A)$, $Y = 2^A$; (iii) X es el conjunto de todas las transformaciones uno a uno de A hacia sí mismo, Y es el conjunto de todos los subconjuntos finitos de A. En cada caso podemos preguntar

cuál de los dos conjuntos X y Y tienen más elementos. El problema es encontrar primero una interpretación rigurosa de la pregunta y después contestarla.

El teorema del buen orden nos dice que todo conjunto puede ser bien ordenado. Para conjuntos bien ordenados tenemos lo que parece ser una medida razonable de su tamaño, a saber, su número ordinal. ¿Resuelven el problema estas dos observaciones? Para comparar los tamaños de X y Y ¿podemos simplemente ordenar cada uno de ellos y después comparar ord X y ord Y? La respuesta es un rotundo no. El problema es que un mismo conjunto puede ser ordenado en muchas formas. El número ordinal de un conjunto bien ordenado mide más al buen ordenamiento que al conjunto. Como un ejemplo concreto considérese al conjunto ω de todos los naturales. Introdúzcase un nuevo orden colocando al cero después de cualquier otra cosa. (En otras palabras, si m y n son números naturales distintos de cero, arréglelos en el orden usual; si, en cambio, $n = 0$ y $m \neq 0$, que m preceda a n). El resultado es un buen ordenamiento de ω y el número ordinal de este buen ordenamiento es $\omega + 1$.

Si X y Y son dos conjuntos bien ordenados, entonces una condición necesaria y suficiente para que ord $X <$ ord Y es que X sea semejante a un segmento inicial de Y. De esto se sigue que podríamos comparar los tamaños ordinales de dos conjuntos bien ordenados aun sin saber nada acerca de números ordinales; todo lo que necesitaríamos conocer es el concepto de semejanza. La semejanza fue definida para conjuntos ordenados y el concepto central para conjuntos no ordenados arbitrarios es el de equivalencia. (Recuérdese que dos conjuntos X y Y son llamados equivalentes, $X \sim Y$, en caso de que exista una correspondencia uno a uno entre ellos).* Si reemplazamos la semejanza por la equivalencia, pasa a ser útil algo como la sugerencia del párrafo precedente. El punto es que no necesitamos saber cuál es el tamaño si todo lo que queremos es comparar los tamaños.

Si X y Y son dos conjuntos tales que X es equivalente a un subconjunto de Y, escribiremos

$$X \precsim Y.$$

La notación es provisional y no amerita un nombre permanente. No obstante, mientras se le use, es conveniente tener una manera de referirse a ella; una posibilidad razonable es

* Véanse notas Págs. 51 y 128.

decir que Y *domina* a X. El conjunto de todas aquellas parejas ordenadas (X, Y) de subconjuntos de algún conjunto E para las cuales $X \precsim Y$ constituye una relación en el conjunto potencia de E. El simbolismo sugiere adecuadamente algunas de las propiedades del concepto que denota. Como el simbolismo es rememorativo de los órdenes parciales y ya que un orden parcial es reflexivo, antisimétrico y transitivo, podemos esperar que la dominación tenga propiedades análogas.

La reflexividad y la transitividad no ocasionan problemas. Ya que cada conjunto X es equivalente a un subconjunto de sí mismo (a saber, X), se sigue que $X \precsim X$ para todo X. Si f es una correspondencia uno a uno entre X y un subconjunto de Y y si g es una correspondencia uno a uno entre Y y un subconjunto de Z, podemos restringir g al rango de f y componer el resultado con f; la conclusión es que X es equivalente a un subconjunto de Z. En otras palabras, si $X \precsim Y$ y $Y \precsim Z$, entonces $X \precsim Z$.

El punto interesante es el de la antisimetría. Si $X \precsim Y$ y $Y \precsim X$, ¿podemos concluir que $X = Y$? Esto es absurdo ya que las suposiciones son satisfechas siempre que X y Y son equivalentes, y conjuntos equivalentes no tienen que ser idénticos. ¿Qué es entonces lo que podemos decir acerca de dos conjuntos si todo lo que sabemos es que cada uno de ellos es equivalente a un subconjunto del otro? La respuesta está contenida en el siguiente célebre e importante resultado.

Teorema de Schröder-Bernstein. *Si $X \precsim Y$ y $Y \precsim X$, entonces $X \sim Y$.*

Observación. Nótese que el recíproco, el cual es incidentalmente un considerable robustecimiento a la afirmación de reflexividad, se sigue trivialmente de la definición del concepto de dominación.

Demostración. Sea f una transformación uno a uno de X hacia Y y sea g una transformación uno a uno de Y hacia X; el problema es construir una correspondencia uno a uno de X *sobre* Y. Es conveniente suponer que los conjuntos X y Y no tienen elementos en común, ya que si esto no sucede, podemos lograrlo tan fácilmente que la suposición adicional no ocasiona pérdida de generalidad.

Diremos que un elemento x de X es el *padre* del elemento $f(x)$ de Y y, análogamente, que un elemento y de Y es el pa-

dre de $g(y)$ de X. Cada elemento x de X tiene una sucesión infinita de *descendientes*, a saber, $f(x)$, $g[f(x)]$, $f[g(f[x])]$, etc., y análogamente, los descendientes de un elemento y de Y son $g(y)$, $f[g(y)]$, $g[f(g[y])]$, etc. Esta definición implica que cada término de la sucesión es un descendiente de todos los términos precedentes; también diremos que cada término de la sucesión es un *ancestro* de todos los términos siguientes.

Para cada elemento (ya sea en X o en Y) debe suceder una de tres cosas. Si nos mantenemos buscando los ancestros del elemento tan anteriores a él como sea posible, llegaremos a un elemento de X que no tiene padre [estos huérfanos son precisamente los elementos de $X - g(Y)$], o bien, llegaremos finalmente a un elemento de Y que no tiene padre $[Y - f(X)]$, o bien, el linaje se remonta al infinito. Sea X_X el conjunto de aquellos elementos de X que se originan en X [o sea, X_X está constituido por los elementos de $X - g(Y)$ junto con todos sus descendientes en X], sea X_Y el conjunto de aquellos elementos de X que se originan en Y [o sea, X_Y está constituido por todos los descendientes en X de los elementos de $Y - f(X)$], y sea X_∞ el conjunto de aquellos elementos de X que no tienen ancestro sin padre. Divídase Y análogamente en los tres conjuntos Y_X, Y_Y y Y_∞.

Si $x \in X_X$, entonces $f(x) \in Y_X$, y, de hecho, la restricción de f a X_X es una correspondencia uno a uno entre X_X y Y_X. Si $x \in X_Y$, entonces x pertenece al dominio de la función inversa g^{-1} y $g^{-1}(x) \in Y_Y$; la restricción de g^{-1} a X_Y es en realidad una correspondencia uno a uno entre X_Y y Y_Y.* Si finalmente, $x \in X_\infty$, entonces $f(x) \in Y_\infty$ y la restricción de f a X_∞ es una correspondencia biunívoca entre X_∞ y Y_∞; alternativamente, si $x \in X_\infty$, entonces $g^{-1}(x) \in Y_\infty$ y la restricción de g^{-1} a X_∞ es una correspondencia uno a uno entre X_∞ y Y_∞. Combinando estas tres correspondencias uno a uno, obtenemos una correspondencia uno a uno entre X y Y.

EJERCICIO. Supóngase que f es una transformación de X hacia Y y g una transformación de Y hacia X. Demuestre que existen subconjuntos A y B de X y Y respectivamente tales

* Aquí *correspondencia uno a uno entre X y Y* significa *sobre* Y en contraposición a correspondencia uno a uno de X en Y o hacia Y que no es necesariamente *sobre* Y. Cabe aclarar que correspondencia o transformación uno a uno es técnicamente sinónimo de correspondencia o *transformación biunívoca.* (N. del R.)

que $f(A) = B$ y $g(Y - B) = X - A$. Este resultado puede ser usado para dar una demostración del teorema de Schröder-Bernstein aparentemente muy distinta de la anterior.

Sabemos ya que la dominación tiene las propiedades esenciales de un orden parcial; concluiremos este estudio introductorio haciendo notar que el orden es de hecho total. La afirmación es conocida como el teorema de la comparabilidad para conjuntos y dice que si X y Y son conjuntos, entonces $X \precsim Y$, o bien, $Y \precsim X$. La demostración es una consecuencia inmediata del teorema del buen orden y del teorema de la comparabilidad para conjuntos bien ordenados. Ordénense bien tanto X como Y y úsese el hecho de que los conjuntos bien ordenados así obtenidos son semejantes, o bien, uno de ellos es semejante a un segmento inicial del otro; en el primer caso X y Y son equivalentes y en el último uno de ellos es equivalente a un subconjunto del otro.

SECCION 23

CONJUNTOS CONTABLES

Si X y Y son conjuntos tales que Y domina a X y X domina a Y, el teorema de Schröder-Bernstein es entonces aplicable y afirma que X es equivalente a Y. Si Y domina a X pero X no domina a Y, de manera que X no es equivalente a Y, escribiremos

$$X \prec Y,$$

y diremos que Y *domina estrictamente* a X.

La dominación y la dominación estricta pueden ser empleadas para expresar en forma concisa algunos hechos acerca de conjuntos finitos e infinitos. Recuérdese que un conjunto X es llamado finito cuando es equivalente a algún número natural; de otra manera es infinito. Sabemos que si $X \precsim Y$ y Y es finito, entonces X es finito, y sabemos que ω es infinito (§ 13); sabemos también que si X es infinito, entonces $\omega \precsim X$ (§ 15). El recíproco de la última proposición es verdadero y puede ser demostrado ya sea directamente (usando el hecho de que un conjunto finito no puede ser equivalente a un subconjunto propio de sí mismo) o como una aplicación del teorema de Schröder-Bernstein. (Si $\omega \precsim X$, entonces es imposible que exista un número natural n tal que $X \sim n$, porque tendríamos $\omega \precsim n$ y esto contradice el hecho de que ω es infinito).

Acabamos de ver que un conjunto X es infinito si y sólo si $\omega \precsim X$; demostraremos en seguida que X es finito si y sólo si $X \prec \omega$. La demostración depende de la transitividad de la dominación estricta: si $X \precsim Y$ y $Y \precsim Z$ y cuando menos una de estas dominaciones es estricta, entonces $X \prec Z$. En realidad, es claro que $X \precsim Z$. Si tuviésemos $Z \precsim X$, entonces deberíamos

tener $Y \precsim X$ y $Z \precsim Y$ y, por consiguiente, (por el teorema de Schröder-Bernstein), $X \sim Y$ y $Y \sim Z$, en contradicción a la suposición de dominación estricta. Si ahora X es finito, entonces $X \sim n$ para algún número natural n y, como ω es infinito, $n \prec \omega$, de manera que $X \prec \omega$. Recíprocamente, si $X \prec \omega$, entonces X debe ser finito, ya que de otra manera tendríamos $\omega \precsim X$, y, por consiguiente, $\omega \prec \omega$, lo cual es absurdo.

Se dice que un conjunto X es *contable* (o *numerable*) cuando $X \precsim \omega$ y que es *infinito contable** cuando $X \sim \omega$. Es claro que un conjunto contable o es finito o es infinito contable. Nuestro principal propósito en la secuela inmediata es hacer ver que muchas construcciones en la teoría de conjuntos realizadas sobre conjuntos contables conducen nuevamente a conjuntos contables.

Comenzaremos con la observación de que todo subconjunto de ω es contable y seguiremos con la deducción de que todo subconjunto de cada conjunto contable es contable. Estos hechos son triviales pero útiles.

Si f es una función de ω *sobre* un conjunto X, entonces X es contable. Para la demostración, obsérvese que para cada x en X el conjunto $f^{-1}(\{x\})$ no es vacío (aquí es donde el carácter *sobre* de f es importante), y consecuentemente, para cada x en X podemos encontrar un número natural $g(x)$ tal que $f(g(x)) = x$. Como la función g es uno a uno de X hacia ω, esto demuestra que $X \precsim \omega$. El lector que se preocupa por tales cosas habrá notado que esta demostración se vale del axioma de la elección, y quizá quiera saber si existe una demostración alternativa que no dependa de ese axioma. (Sí la hay). El mismo comentario es aplicable en algunas otras ocasiones, tanto de esta sección como de las siguientes, pero nos abstendremos de hacerlo.

Se sigue del párrafo precedente que un conjunto X es contable si y sólo si existe alguna función de algún conjunto contable sobre X. Un resultado estrechamente ligado es éste: si Y es cualquier conjunto particular infinito contable, entonces una condición necesaria y suficiente para que un conjunto X no vacío sea contable es que exista una función de Y sobre X.

La función $n \to 2n$ es una correspondencia uno a uno entre ω y el conjunto A de todos los números pares, de manera que

* La traducción literal original es "*contablemente infinito*" (N. del T.)

A es infinito contable. Esto implica que si X es un conjunto contable, entonces existe una función f que transforma a A sobre X. Ya que, análogamente, $n \to 2n + 1$ es una correspondencia uno a uno entre ω y el conjunto B de todos los números nones, se sigue que si Y es un conjunto contable, entonces existe una función g que transforma a B sobre Y. La función h que coincide con f en A y con g en B (esto es, $h(x) = f(x)$ cuando $x \in A$ y $h(x) = g(x)$ cuando $x \in B$) transforma a ω sobre $X \cup Y$. Conclusión: la unión de dos conjuntos contables es contable. De aquí en adelante un sencillo proceso demuestra por inducción matemática que la unión de un conjunto finito de conjuntos contables es contable. El mismo resultado puede ser obtenido si se imita el artificio que funcionó para el caso de dos conjuntos; la base del método es el hecho de que para cada número natural n distinto de cero existe una familia $\{A_i\}$ $(i < n)$ de subconjuntos infinitos ajenos entre sí de ω cuya unión es igual a ω.

El mismo método puede ser usado para demostrar aún más cosas. Afirmación: existe una familia $\{A_n\}$ $(n \in \omega)$ de subconjuntos infinitos ajenos de ω cuya unión es igual a ω. Una manera de demostrar esto es escribiendo los elementos de ω en un arreglo infinito siguiendo las diagonales, así:

$$\begin{array}{rrrrrrr} 0 & 1 & 3 & 6 & 10 & 15 & \cdots \\ 2 & 4 & 7 & 11 & 16 & \cdots & \\ 5 & 8 & 12 & 17 & \cdots & & \\ 9 & 13 & 18 & \cdots & & & \\ 14 & 19 & \cdots & & & & \\ 20 & \cdots & & & & & \end{array}$$

y considerar después la sucesión de las filas de este arreglo. Otra manera es tomar A_0 como constituido por 0 y por los números nones, A_1 obtenido al duplicar a cada elemento distinto de cero de A_0 e, inductivamente, sea A_{n+1} el conjunto obtenido al duplicar cada elemento de A_n, $n \geqq 1$. Cualquiera que sea el método (y hay aún muchos otros) los detalles son fáciles de cubrir. Conclusión: la unión de una familia infinita contable de conjuntos contables es contable. Demostración: dada la familia $\{X_n\}$ $(n \in \omega)$ de conjuntos contables, encuéntrese una familia $\{f_n\}$ de funciones tales que, para cada n, la función f_n

* Correspondencia uno a uno o biunívoca. (N. del R.)

transforma a A_n sobre X_n y defínase una función f de ω sobre $\bigcup_n X_n$ escribiendo $f(k) = f_n(k)$ siempre que $k \in A_n$. Este resultado en combinación con el del párrafo precedente implica que la unión de un conjunto contable de conjuntos contables es siempre contable.

Como un corolario interesante y útil tenemos que el producto cartesiano de dos conjuntos contables es contable también. Como

$$X \times Y = \bigcup_{y \in Y} (X \times \{y\}),$$

y ya que si X es contable, entonces para cada y de Y, fija, el conjunto $X \times \{y\}$ es obviamente contable (empléese la correspondencia biunívoca $x \to (x, y)$), el resultado se sigue del párrafo precedente.

EJERCICIO. Demuestre que el conjunto de todos los subconjuntos finitos de un conjunto contable es contable. Demuestre que si todo subconjunto contable de un conjunto X totalmente ordenado está bien ordenado, entonces X mismo está bien ordenado.

Sobre la base del estudio precedente no sería insensato suponer que todo conjunto es contable. Procederemos a ver que no es así, y este resultado negativo es lo que hace interesante la teoría de los números cardinales.

Teorema de Cantor. *Todo conjunto está estrictamente dominado por su conjunto potencia, o, en otras palabras.*

$$X \prec \mathcal{P}(X)$$

para todo X.

DEMOSTRACIÓN. Hay una correspondecia biunívoca de X hacia $\mathcal{P}(X)$, a saber, la que asocia a cada elemento x de X el conjunto singular $\{x\}$. La existencia de esta función demuestra que $X \precsim \mathcal{P}(X)$; falta demostrar que X no es equivalente a $\mathcal{P}(X)$.

Supóngase que f es una transformación uno a uno de X sobre $\mathcal{P}(X)$; nuestro propósito es hacer ver que esta suposición conduce a una contradicción. Escríbase $A = \{x \in X : x \in' f(x)\}$; en palabras, A está constituido por aquellos elementos de X que no están contenidos en el conjunto correspondiente. Como $A \in \mathcal{P}(X)$ y ya que f transforma a X sobre $\mathcal{P}(X)$, existe un elemento a en X tal que $f(a) = A$. El elemento a, o pertenece al conjunto

A o no pertenece a él. Si $a \in A$, entonces, por la definición de A, debemos tener $a \in' f(a)$, y como $f(a) = A$ esto es imposible. Si $a \in' A$, entonces, otra vez por la definición de A, debemos tener $a \in f(a)$, y esto también es imposible. La contradicción ha llegado y la demostración del teorema de Cantor está terminada.

Como $\mathcal{P}(X)$ es siempre equivalente a 2^X (donde 2^X es el conjunto de todas las funciones de X hacia 2), el teorema de Cantor implica que $X \prec 2^X$ para todo X. Si tomamos en particular a ω en el papel de X, entonces podemos llegar a la conclusión de que el conjunto de todos los conjuntos de números naturales es *incontable* (esto es, no contable, no numerable) o, en forma equivalente, que 2^ω es incontable. Aquí, 2^ω representa al conjunto de todas las sucesiones infinitas de ceros y unos (o sea, las funciones de ω hacia 2). Obsérvese que si interpretamos a 2^ω como exponenciación ordinal, entonces 2^ω es contable (de hecho $2^\omega = \omega$).

SECCION 24

ARITMETICA CARDINAL

Un resultado de nuestro estudio de los tamaños comparativos de los conjuntos será el de definir un nuevo concepto, llamado *número cardinal* y asociar con cada conjunto X un número cardinal denotado por card X. Las definiciones son tales que para cada número cardinal a existen conjuntos A con card $A = a$. También definiremos un orden para los números cardinales, denotado como es usual por $\leqq$. La conexión entre estos nuevos conceptos y los que ya están a nuestra disposición es fácil de describir: sucederá que card X = card Y si y sólo si $X \sim Y$, y card $X <$ card Y si y sólo si $X \prec Y$. (Si a y b son números cardinales, $a < b$ significa, por supuesto, que $a \leqq b$ pero $a \neq b$.)

La definición de números cardinales puede ser introducida de muy diversas maneras, cada una de las cuales tiene fuertes partidarios. Con el fin de conservar la paz mientras sea posible y demostrar que las propiedades esenciales del concepto son independientes de la vía de entrada, pospondremos la construcción básica. Procederemos, en cambio, a estudiar la aritmética de los números cardinales. A lo largo de este estudio vamos a hacer uso de la conexión descrita anteriormente, entre la desigualdad cardinal y la dominación entre conjuntos; ese anticipo de lo que vendrá más adelante será suficiente para el propósito.

Si a y b son números cardinales y si A y B son conjuntos ajenos con card $A = a$ y card $B = b$, escribiremos, por definición, $a + b$ = card $(A \cup B)$. Si C y D son dos conjuntos ajenos con card $C = a$ y card $D = b$, entonces $A \sim C$ y $B \sim D$; se sigue que $A \cup B \sim C \cup D$ y, por consiguiente, que $a + b$ está bien definido, es decir independientemente de la elección

arbitraria de A y B. La adición cardinal, así definida, es conmutativa $(a + b = b + a)$ y asociativa $[a + (b + c) = (a + b) + c]$, siendo estas identidades consecuencias inmediatas de las propiedades correspondientes acerca de la formación de uniones.

EJERCICIO. Demuestre que si a, b, c y d son números cardinales tales que $a \leqq b$ y $c \leqq d$, entonces $a + c \leqq b + d$.

No hay dificultad alguna para definir la adición para un número infinito de sumandos. Si $\{a_i\}$ es una familia de números cardinales y $\{A_i\}$ una familia con igual conjunto de índices, de conjuntos mutuamente ajenos tal que card $A_i = a_i$ para cada i. entonces, por definición, escribiremos

$$\sum_i a_i = \text{card } (\bigcup_i A_i).$$

Como antes, la definición no presenta ambigüedades.

Para definir el producto ab de dos números cardinales a y b, encontramos dos conjuntos A y B con card $A = a$ y card $B = b$ y escribimos $ab =$ card $(A \times B)$. El reemplazo de A y B por conjuntos equivalentes conduce al mismo valor del producto. Alternativamente, pudimos haber definido ab como "la adición de a consigo mismo b veces", lo cual se refiere a la formación de la suma infinita $\sum_{i \in I} a_i$, donde el conjunto de índices I, tiene número cardinal b y donde $a_i = a$ para cada i de I. El lector no debe tener dificultad en verificar que esta definición alternativa propuesta es en realidad equivalente a la que emplea productos cartesianos. La multiplicación cardinal es conmutativa $(ab = ba)$ y asociativa $[a, (bc) = (ab)c]$ y distribuye a la adición $[a(b + c) = ab + ac]$; las demostraciones son elementales.

EJERCICIO. Demuestre que si a, b, c y d son números cardinales tales que $a \leqq b$ y $c \leqq d$, entonces $ac \leqq bd$.

No hay dificultad alguna en definir la multiplicación para un número infinito de factores. Si $\{a_i\}$ es una familia de números cardinales y $\{A_i\}$ una familia con igual conjunto de índices, de conjuntos tal que card $A_i = a_i$ para cada i, entonces, por definición, escribimos

$$\prod_i a_i = \text{card } (\times_i A_i)$$

La definición carece de ambigüedad.

EJERCICIO. Si $\{a_i\}$ $(i \in I)$ y $\{b_i\}$ $(i \in I)$ *son* familias de números cardinales tales que $a_i < b_i$ para cada i de I, entonces $\sum_i a_i < \prod_i b_i$.

Podemos ir de productos a exponentes de la misma manera en que fuimos de sumas a productos. La definición de a^b, para números cardinales a y b resulta más provechosa cuando se da directamente, pero una vía de entrada alternativa es a través de la multiplicación repetida. Para la definición directa, encuéntrense conjuntos A y B con card $A = a$ y card $B = b$ y escríbase $a^b =$ card A^B. Alternativamente, para definir a^b "multiplíquese a por sí mismo b veces". Más precisamente: fórmese $\prod_{i \in I} a_i$, donde el conjunto de índices I tiene número cardinal b y donde $a_i = a$ para cada i de I. Las leyes usuales para exponentes se cumplen. Esto es, si a, b y c son números cardinales, entonces

$$a^{b+c} = a^b a^c,$$

$$(ab)^c = a^c b^c,$$

$$a^{bc} = (a^b)^c.$$

EJERCICIO. Demuestre que si a, b y c son números cardinales, tales que $a \leqq b$, entonces $a^c \leqq b^c$. Demuestre que si a y b son finitos, mayores que 1, y c infinito, entonces $a^c = b^c$.

Las definiciones precedentes y sus consecuencias son razonablemente directas y nada sorprendentes. Si son restringidas a conjuntos finitos solamente, el resultado es la conocida aritmética finita. La innovación de lo expuesto consiste en la formación de sumas, productos y potencias en las cuales cuando menos un término es infinito. Las palabras "finito" e 'infinito" son empleadas aquí en un sentido muy natural: un número cardinal es *finito* si es el número cardinal de un conjunto finito; de otra manera es *infinito*.

Si a y b son números cardinales tales que a es finito y b infinito, entonces

$$a + b = b.$$

Para la demostración, supóngase que A y B son dos conjuntos mutuamente ajenos tales que A es equivalente a algún número natural k y B es infinito; debemos demostrar que $A \cup B \sim B$. Como $\omega \precsim B$, podemos suponer, y lo hacemos, que $\omega \subset B$. Definimos

una función f de $A \cup B$ a B en la forma siguiente: la restricción de f a A es una correspondencia uno a uno entre A y k, la restricción de f a ω está dada por $f(n) = n + k$ para todo n y la restricción de f a $B - \omega$ es la función identidad en $B - \omega$. Ya que el resultado es una correspondencia uno a uno entre $A \cup B$ y B, la demostración está completa.

En seguida: si a es un número cardinal infinito, entonces

$$a + a = a.$$

Para la demostración, sea A un conjunto con card $A = a$. Ya que el conjunto $A \times 2$ es la unión de dos conjuntos ajenos equivalentes a A (a saber, $A \times \{0\}$ y $A \times \{1\}$), será suficiente demostrar que $A \times 2$ es equivalente a A. La vía de entrada que emplearemos no demostrará esto completamente, pero se acercará lo suficiente. La idea es aproximar la construcción de la correspondencia uno a uno deseada empleando subconjuntos de A cada vez mayores.

Hablando precisamente, sea $\mathfrak{F}$ la colección de todas las funciones f tales que el dominio de f es de la forma $X \times 2$, para algún subconjunto X de A, siendo cada f una correspondencia uno a uno entre $X \times 2$ y X. Si X es un subconjunto infinito contable de A, entonces $X \times 2 \sim X$. Esto implica que la colección $\mathfrak{F}$ no es vacía; por lo menos contiene a las correspondencias uno a uno entre $X \times 2$ y X para los subconjuntos X infinitos contables de A. La colección $\mathfrak{F}$ está parcialmente ordenada por extensión. Como una verificación directa deja ver que la hipótesis del lema de Zorn se satisface, se sigue que $\mathfrak{F}$ contiene, digamos, un máximo elemento f con ran $f = X$.

Afirmación: $A - X$ es finito. Si $A - X$ fuera infinito, incluiría un conjunto infinito contable, digamos Y. Combinando f con una correspondencia uno a uno entre $Y \times 2$ y Y podríamos obtener una extensión propia de f, en contradicción con el supuesto de que f es elemento máximo.

Ya que card X + card X = card X y puesto que card A = card X + card $(A - X)$, el hecho de que $A - X$ es finito completa la demostración de que card A + card A = card A.

He aquí un resultado más de la aritmética cardinal aditiva: si a y b son números cardinales tales que cuando menos uno de ellos es infinito y si c es igual al mayor de entre a y b, entonces

$$a + b = c.$$

Supóngase que b es infinito y sean A y B conjuntos mutuamente ajenos con card $A = a$ y card $B = b$. Como $a \leqq c$ y $b \leqq c$, se sigue que $a + b \leqq c + c$ y como $c \leqq$ card $(A \cup B)$, se sigue que $c \leqq a + b$. El resultado emana de la antisimetría del ordenamiento de los números cardinales.

El principal resultado de la aritmética cardinal multiplicativa es que si a es un número cardinal infinito, entonces

$$a \cdot a = a.$$

La demostración se asemeja a la de la propiedad correspondiente de la adición. Sea $\mathfrak{F}$ la colección de todas las funciones f, tales que el dominio de f sea de la forma $X \times X$ para algún subconjunto X de A siendo cada f una correspondencia uno a uno entre $X \times X$ y X. Si X es un subconjunto infinito contable de A, entonces $X \times X \sim X$. Esto implica que la colección $\mathfrak{F}$ no es vacía, ya que cuando menos contiene a las correspondencias uno a uno entre $X \times X$ y X para los subconjuntos X infinitos contables de A. La colección $\mathfrak{F}$ está parcialmente ordenada por extensión. Las hipótesis del lema de Zorn son verificadas fácilmente, y se sigue que $\mathfrak{F}$ contiene un elemento máximo f con ran $f = X$. Como (card X) (card X) = card X, la demostración puede completarse haciendo ver que card X = card A.

Supóngase que card $X <$ card A. Ya que card A es igual al mayor de entre card X y card $(A - X)$, esto implica que card A = card $(A - X)$ y, por consiguiente, que card $X <$ card $(A - X)$. De esto se sigue que $A - X$ tiene un subconjunto Y equivalente a X. Ya que cada uno de los conjuntos ajenos $X \times Y$, $Y \times X$ y $Y \times Y$ es infinito y equivalente a $X \times X$ y por lo tanto a X y a Y, se sigue que su unión es equivalente a Y. Combinando f con una correspondencia uno a uno entre esa unión y Y, obtenemos una extensión propia f, en contradicción a lo supuesto. Esto implica que nuestra presente hipótesis (card $X <$ card A) es insostenible, lo cual completa la demostración.

Ejercicio. Demuestre que si a y b son números cardinales tales que cuando menos uno de ellos es infinito, entonces $a + b = ab$. Demuestre que si a y b son números cardinales tales que a es infinito y b finito, entonces $a^b = a$.

SECCION 25

NUMEROS CARDINALES

Ya sabemos bastante acerca de números cardinales, pero aún no sabemos lo que son. Hablando vagamente, podemos decir que el número cardinal de un conjunto es la propiedad común que tienen el conjunto y todos los conjuntos equivalentes a él. Podemos tratar de hacer esto preciso diciendo que el número cardinal de X es igual al conjunto de todos los conjuntos equivalentes a X, pero el intento fallará ya que no hay un conjunto así de grande. Lo siguiente a ensayar, sugerido por la analogía con nuestra vía de entrada a la definición de los números naturales, es definir al número cardinal de un conjunto X como un conjunto equivalente a X elegido en forma particularmente cuidadosa. Esto es lo que procederemos a hacer.

Para cada conjunto X hay muchos conjuntos equivalentes a X; nuestro primer problema es reducir el campo. Como sabemos que todo conjunto es equivalente a algún número ordinal, no es antinatural buscar los conjuntos típicos, los conjuntos representativos, entre los números ordinales.

Indudablemente, un conjunto puede ser equivalente a muchos números ordinales. Sin embargo, una señal prometedora es el hecho de que, para cada conjunto X, los números ordinales equivalentes a X constituyen un conjunto. Para demostrar esto, obsérvese primero que es fácil producir un número ordinal que sea seguramente mayor, estrictamente mayor, que todos los números ordinales equivalentes a X. Supóngase de hecho que γ es un número ordinal equivalente al conjunto potencia $\mathcal{P}(X)$. Si α es un número ordinal equivalente a X, entonces el conjunto α está estrictamente dominado por el con-

junto γ (esto es, card $\alpha <$ card γ). Se sigue que no podemos tener $\gamma \leqq \alpha$ y, en consecuencia, debemos tener $\alpha < \gamma$. Ya que, para números ordinales, $\alpha < \gamma$ significa lo mismo que $\alpha \in \gamma$, hemos encontrado un conjunto, a saber, γ, que contiene a todo número ordinal equivalente a X, lo cual implica que los números ordinales equivalentes a X constituyen en efecto un conjunto.

¿Cuál de entre los números ordinales equivalentes a X merece ser singularizado y llamado número cardinal de X? La pregunta tiene sólo una respuesta natural. Todo conjunto de números ordinales está bien ordenado y el primer elemento de un conjunto bien ordenado es el único que parece reclamar atención especial.

Ahora estamos preparados para la definición: un *número cardinal* es un número ordinal α tal que si β es un número ordinal equivalente a α (esto es, card $\alpha =$ card β), entonces $\alpha \leqq \beta$. Los números ordinales con esta propiedad también han sido llamados *números iniciales*. Si X es un conjunto, entonces card X, el número cardinal de X (también conocido como la *potencia de* X), es el primer número ordinal equivalente a X.

EJERCICIO. Demuestre que cada número cardinal infinito es un número límite.

Ya que cada conjunto es equivalente a su número cardinal, se sigue que si card X = card Y, entonces X ~ Y. Si, recíprocamente, X ~ Y, entonces card X ~ card Y. Como card X es el primer número ordinal equivalente a X, se sigue que card X $\leqq$ card Y, y, ya que la situación es simétrica en X y Y, también tenemos que card Y $\leqq$ card X. En otras palabras, card X = card Y si y sólo si X ~ Y; ésta era una de las condiciones sobre números cardinales necesaria para el desarrollo de la aritmética cardinal.

Un número ordinal finito (esto es, un número natural) no es equivalente a ningún número ordinal finito distinto de sí mismo. Se sigue que si X es finito, el conjunto de los números ordinales equivalentes a X es un conjunto singular y, en consecuencia, el número cardinal de X es lo mismo que el número ordinal de X. Tanto los números cardinales como los ordinales son generalizaciones de los números naturales; en los casos finitos usuales ambas generalizaciones coinciden con el caso especial que las originó. Como una aplicación casi trivial de estas observaciones, podemos calcular ahora el número cardinal de

un conjunto potencia $\mathcal{P}(A)$: si card $A = a$, entonces card $\mathcal{P}(A) = 2^a$. (Obsérvese que el resultado, aunque simple, no pudo haber sido establecido antes de esto, hasta ahora no sabíamos que 2 es un número cardinal.) La demostración es inmediata a partir del hecho de que $\mathcal{P}(A)$ es equivalente a 2^A.

Si α y β son números ordinales, sabemos lo que significa decir que $\alpha < \beta$ o $\alpha \leqq \beta$. Se sigue que los números cardinales vienen a nosotros acompañados automáticamente de un orden. El orden satisface las condiciones que tomamos como anticipo para nuestro estudio de aritmética cardinal. En realidad: si card $X <$ card Y, entonces card X es un subconjunto de card Y y se sigue que $X \precsim Y$. Si tuviésemos $X \sim Y$, entonces, como hemos visto ya, card X = card Y y se sigue que debemos tener $X \prec Y$. Finalmente, si $X \prec Y$, es imposible que card $Y \leqq$ card X (y a que la semejanza implica equivalencia) y, por lo tanto, card $X <$ card Y.

Como una aplicación de estas consideraciones mencionaremos la desigualdad

$$a < 2^a,$$

válida para todos los números cardinales a. Demostración: si A es un conjunto con card $A = a$, entonces $A \prec \mathcal{P}(A)$, de manera que card $A <$ card $\mathcal{P}(A)$, por lo tanto, $a < 2^a$.

EJERCICIO. Si card $A = a$ ¿cuál es el número cardinal del conjuntos de todas las funciones uno a uno de A sobre sí mismo? ¿Cuál es el número cardinal del conjunto de todos los subconjuntos infinitos contables de A?

Las propiedades acerca del ordenamiento de los números ordinales son a la vez propiedades del ordenamiento de los números cardinales. Así, por ejemplo, sabemos que dos números cardinales cualesquiera son comparables (siempre sucede que $a < b$ o $a = b$ o $b < a$) y que, en realidad, todo conjunto de números cardinales está bien ordenado. Sabemos también que todo conjunto de números cardinales tiene una cota superior (de hecho, un supremo) y que, más aún, para cada conjunto de números cardinales, hay un número cardinal estrictamente mayor que cualquiera de ellos. Por supuesto, esto implica que no hay un número cardinal mayor que cualquier otro número cardinal o equivalentemente, que no hay un conjunto constituido

precisamente por todos los números cardinales. La contradicción, basada en la suposición de que existe tal conjunto es conocida como la *paradoja de Cantor*.

El hecho de que los números cardinales son números ordinales especiales simplifica algunos aspectos de la teoría, pero, a la vez, introduce la posibilidad de cierta confusión que es esencial eliminar. Una fuente de dificultades es la notación para las operaciones aritméticas. Si a y b son números cardinales, entonces también son números ordinales y, en consecuencia, la suma $a + b$ tiene dos significados posibles. La suma cardinal de dos números cardinales no es en general lo mismo que su suma ordinal. Todo esto parece peor de lo que es, ya que en la práctica es fácil eliminar la confusión. El contexto, el uso de símbolos especiales para números cardinales y una advertencia explícita ocasional pueden hacer que el estudio fluya suavemente y sin obstáculos.

EJERCICIO. Demuestre que si α y β son números ordinales, entonces card $(\alpha + \beta) =$ card $\alpha +$ card β y card $(\alpha\beta) =$ (card α) (card β). Emplee la interpretación ordinal de las operaciones en los miembros de la izquierda y la cardinal en los de la derecha.

Uno de los símbolos especiales para números cardinales que es usado con mucha frecuencia es la primera letra del alfabeto hebreo ($\aleph$, álef). Así en particular, el número ordinal transfinito más chico, esto es, ω, es un número cardinal y, como tal, es denotado siempre por $\aleph_0$.

Cada uno de los números ordinales que hemos nombrado explícitamente hasta ahora es contable. En muchas de las aplicaciones de la teoría de los conjuntos, el número ordinal incontable más chico, frecuentemente denotado por Ω, juega un papel importante. La propiedad más importante de ω es que es un conjunto infinito bien ordenado, cada uno de cuyos segmentos iniciales es finito y la propiedad correspondiente más importante de Ω es que es un conjunto bien ordenado infinito incontable, cada uno de cuyos segmentos iniciales es contable.

El primer número ordinal incontable Ω satisface en forma clara la condición que define a un número cardinal, y en su aspecto cardinal siempre es denotado por $\aleph_1$. En forma equivalente, $\aleph_1$, puede ser caracterizado como el primer número cardinal estrictamente mayor que $\aleph_0$ o, en otras palabras, el

sucesor inmediato de $\aleph_0$ en el ordenamiento de los números cardinales.

La relación aritmética entre $\aleph_0$ y $\aleph_1$ es el tema de un viejo y famoso problema acerca de los números cardinales. ¿Cómo pasamos de $\aleph_0$ a $\aleph_1$ por medio de operaciones aritméticas? Sabemos ya que los pasos más elementales, constituidos por sumas y productos, solamente conducen de $\aleph_0$ otra vez a $\aleph_0$. Lo más sencillo que sabemos hacer que comienza con $\aleph_0$ y desemboca a algo más grande es la formación de $2^{\aleph_0}$. Sabemos entonces que $\aleph_1 \leqq 2^{\aleph_0}$ ¿Es estricta la desigualdad? ¿Existe un número cardinal incontable estrictamente menor que $2^{\aleph_0}$? La célebre ***hipótesis del continuo*** afirma, en calidad de conjetura, que la respuesta es no o, en otras palabras, que $\aleph_1 = 2^{\aleph_0}$. Todo lo que se sabe de seguro es que la hipótesis del continuo es consistente con los axiomas de la teoría de los conjuntos.

Para cada número cardinal a, considérese el conjunto $c(a)$ de todos los números cardinales infinitos que son estrictamente menores que a. Si $a = \aleph_0$, entonces $c(a) = \varnothing$; si $a = \aleph_1$, entonces $c(a) = \{\aleph_0\}$. Como $c(a)$ es un conjunto bien ordenado, tiene un número ordinal, digamos α. La conexión entre a y α es expresada usualmente escribiendo $a = \aleph_\alpha$. Una definición equivalente de los números cardinales $\aleph_\alpha$ procede por inducción transfinita; de acuerdo con esa vía de entrada, $\aleph_\alpha$ (para $\alpha > 0$) es el número cardinal más chico que es estrictamente mayor que todos los $\aleph_\beta$'s con $\beta < \alpha$. La *hipótesis del continuo generalizada* es la conjetura de que $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$ para cada número ordinal α.

INDICE

Dr. Salcedo Ecopda



5-82-51-73

Victor Hugo Cerecedo

ESTA IMPRESION DE 2,000 EJEMPLARES
SE TERMINO EL 5 DE ABRIL DE 1973,
EN LOS TALLERES DE LA CÍA. EDITORIAL
CONTINENTAL, S. A., MEXICO

TEORIA INTUITIVA* DE LOS CONJUNTOS

Por Paul R. Halmos

Los matemáticos están de acuerdo en que cada uno de ellos debe saber algo sobre la teoría de conjuntos; el desacuerdo comienza al tratar de decidir qué tanto es algo. Este libro contiene la respuesta a esa pregunta. Su propósito es el de comunicar al principiante en matemáticas avanzadas los hechos básicos en la vida acerca de la teoría de los conjuntos, y hacerlo con un mínimo de raciocinio filosófico y formalismo lógico. El punto de vista, de principio a fin, es el de un futuro matemático ansioso de estudiar grupos, integrales o variedades. Desde ese punto de vista, los conceptos y métodos de este libro son tan sólo algunas de las herramientas usuales de las matemáticas; el especialista experto no encontrará nada nuevo aquí.

En lugar de *Teoría Intuitiva de los Conjuntos*, un título más honrado para el libro habría sido Un Esbozo de los Elementos de la Teoría Intuitiva de los Conjuntos. La palabra "elementos" dejaría ver al lector que no todo se incluye aquí, y la palabra "esbozo" lo prevendría en el sentido de que aun lo que se incluye necesita ser completado.

El estilo es usualmente informal, con objeto de beneficiar la conversación. Se presentan muy pocos teoremas. La mayoría de los hechos sólo son propuestos y van seguidos de un bosquejo de demostración, en forma muy parecida a como lo estarían en una lectura descriptiva general. Hay sólo unos cuantos ejercicios señalados expresamente como tales pero, de hecho, la mayor parte del libro no es otra cosa que una larga cadena de ejercicios con sugerencias. El lector debe preguntarse continuamente a sí mismo si está o no en condiciones de pasar de una sugerencia a la siguiente y, en relación a ello, no debe desanimarse si encuentra que su rapidez de asimilación es más baja que la acostumbrada.

* En el original aparece *Naïve*, que significa ingenua o cándida.